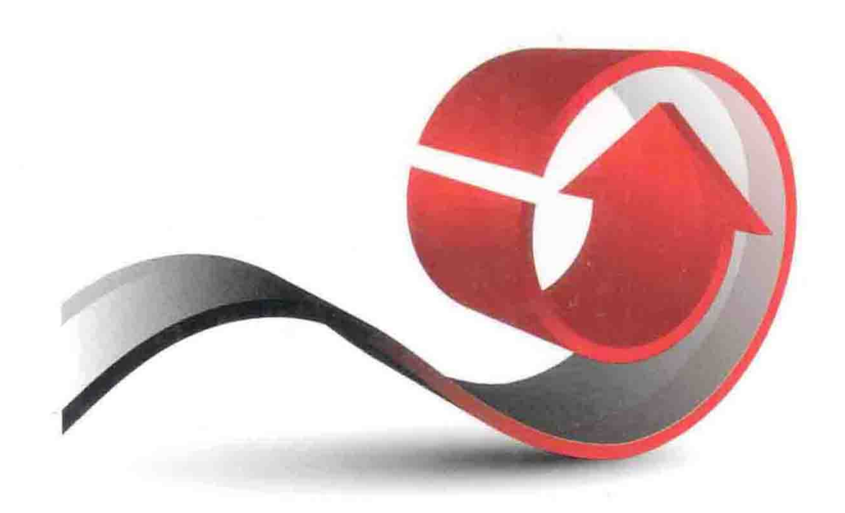


> 华为ICT认证系列丛书

华为路由器学习指南

王达 主编



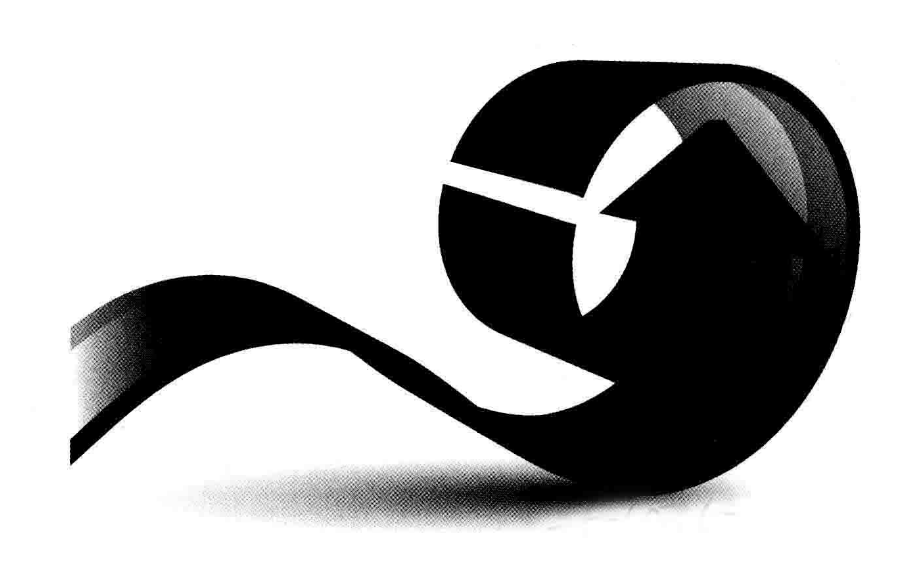




> 华为ICT认证系列丛书

华为路由器学习指南

王达 主编



人民邮电出版社

北京

图书在版编目（CIP）数据

华为路由器学习指南 / 王达主编. -- 北京 : 人民邮电出版社, 2014.8
（华为ICT认证系列丛书）
ISBN 978-7-115-35742-7

Ⅰ. ①华… Ⅱ. ①王… Ⅲ. ①计算机网络－路由选择－指南 Ⅳ. ①TN915.05-62

中国版本图书馆CIP数据核字(2014)第109626号

内 容 提 要

本书是国内图书市场第一本，也是目前为止唯一一本专门介绍华为路由器配置与管理的权威工具图书，同时也是华为技术有限公司指定的 ICT 认证系列培训教材。全书共分三篇、15 章。第一篇：路由器选型及基本功能配置与管理，具体包括 AR G3、NE 系列路由器的选型及应用，各种登录方式/启动系统/BootROM 菜单/信息中心/U 盘开局/自动配置，各种路由器接口（特别是各种 WAN 接口）、WAN 接入与互联、DHCP/DNS 服务、NAT 等功能的配置与管理。第二篇：可靠性配置与管理，具体包括 BFD/NQA、VRRP、接口备份和双机热备份等功能的配置与管理。第三篇：路由配置与管理，具体包括静态路由、RIP 路由、OSPF 路由、IS-IS 路由、BGP 路由，以及路由策略和策略路由的配置与管理。

本书结合了笔者 20 多年的工作经验，其内容非常全面、系统，对每章所介绍的技术原理及基础知识进行了全面、深入的剖析与讲解，并在介绍完每一功能的配置后还有大量的综合配置案例加以巩固。因此，本书无论在专业性方面，还是在经验性和实用性方面均有很好的保障，是相关人员自学或者教学华为路由器配置与管理内容的必选教材。

◆ 主　　编　王　达
责任编辑　李　静
责任印制　杨林杰

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：787×1092　1/16
印张：64.5　　2014 年 8 月第 1 版
字数：1529 千字　　2014 年 8 月北京第 1 次印刷

定价：149.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

人类社会和人类文明发展的历史也是一部科学技术发展的历史。半个多世纪以来，精彩纷呈的ICT技术，汇聚成了波澜壮阔的互联网，突破了时间和空间的限制，把人类社会和人类文明带入到前所未有的高度。今天，人类社会已经步入网络和信息时代，我们已经处在无处不在的网络连接中，连接已经成为一种常态，信息浪潮迅速而深刻地改变着我们的工作和生活。人们与世界连接得如此紧密，实现了随时随地自由沟通，对信息与数据的获取、分享也唾手可得。这意味着，这个连接的世界，正以超乎想象的速度与力量，对人类社会的政治经济、商业文明和生产方式等进行全面的重塑。

ICT正在蓬勃发展，移动性、云计算、大数据和社区化等新趋势正在引领行业开创新的格局；世界正在发生影响深远的数字化变革，互联网正在促进传统产业的升级和重构；通过以业务、用户和体验为中心的敏捷网络架构将深刻影响着未来数字社会的基础。我们深知每个人都拥有平等的数字发展机会，这对于构建一个更加公平的现实世界至关重要。

ICT产业的发展离不开人才的支撑，产业的变革也将对ICT行业人才的知识体系和综合技能提出更高的挑战。作为全球领先的信息与通信解决方案供应商，华为的产品与解决方案已广泛应用于金融、电力、能源、交通、企业、运营商、政府等各个行业。同时，我们也非常注重对ICT专业人才的培养。所以，我们与行业专家、高校老师合作编写了“华为ICT认证系列丛书”，旨在为广大用户、ICT从业者，以及愿意投身到ICT行业中的人士提供学习帮助。

《华为交换机学习指南》的出版发行之后，得到广大读者的高度关注和大力支持，并且读者非常期待华为路由器相关书籍的出版发行。为此，我们再度与国内资深网络技术专家、业界知名作者——王达老师合作并出版《华为路由器学习指南》一书。这本书是从学习和实用的角度，基于学习的逻辑对知识点进行了系统地组织编排，书籍由浅入深，让读者逐步构建起系统的网络知识体系；同时该书在内容上注重理论和实践相结合，既有原理讲解，又有配置应用，让读者能够学以致用。希望本书能够帮助读者快速地学习华为产品技术，系统地建立网络知识体系，使读者在浩瀚的知识海洋中找到方向，不断提升，在ICT行业大展身手！

交换机与企业通信产品线总裁

华为技术有限公司

2014年5月

自　　序

本书出版背景

笔者与华为技术有限公司和人民邮电出版社合作出版的第一本华为设备著作——《华为交换机学习指南》自2014年年初成功上市以来，得到了华为技术有限公司官方，以及全国华为设备用户、华为认证培训机构、华为公司合作伙伴和许许多多读者的高度关注与大力支持。由此可以明显感受到，华为设备用户和广大读者朋友对于学习华为设备，索求系统、权威学习资料的急切需求。在此对所有关注与支持这两本图书的各界朋友，特别是读者朋友表示我最由衷的感谢！

为了能为全国华为设备用户和急切想学习华为设备知识的广大读者朋友提供更全面的权威学习资料，笔者决定再度与华为技术有限公司和人民邮电出版社进行合作，联手推出《华为路由器学习指南》这本图书。其实，许多读者也通过各种渠道（如笔者的10多个专门的读者QQ群、笔者的微博等）早已获知本书即将出版的消息，笔者也经常收到读者朋友关于本书出版情况的询问，并表示"一上市，马上购买"。在此真诚地对你们说声"谢谢！"。

大家或许已经从《华为交换机学习指南》这本书中明显感受到本系列丛书的高起点、大制作的气魄，因为本书不仅有数十位资深网络技术专家参与编写，更有华为技术有限公司官方诸多一线产品专家的严格审核和技术把关，当然还有人民邮电出版社许多编辑老师的多次审核，所以本书无论从专业性、实用性，还是从图书编排、出版质量上都有着非一般图书可比的全线保障。在此可以告诉大家一个好消息，在笔者为本书作序时，《华为交换机学习指南》一书即将进行第一次重印，而这离这本图书正式在各大书店上架还不到两个月的时间。本次出版的《华为路由器学习指南》同样采用这种编写和出版模式，在图书各方面及质量上同样得到全面保障，敬请大家放心选购。

服务与支持

本书得到了华为技术有限公司的许多专家的大力帮助与指导，并由他们进行了全书内容的正确性和权威性的审核，同时也得到了人民邮电出版社各位编辑老师的支持，在此代表全体编委成员一并表示最由衷的感谢！

由于编者水平有限，编写时间比较紧，因此尽管我们全体编写人员和出版社编辑老师花了大量的时间和精力校验，但书中仍可能存在一些错误和瑕疵，敬请各位批评指正，万分感谢！大家可以通过以下渠道向我们反馈，提出你的宝贵意见。同时我们也将通过以下渠道为大家提供专业的服务：

1．5个分片的超级QQ读者群（仅允许对应加入一个群）

华北地区（包括黑龙江、吉林、辽宁、内蒙古、北京、天津、河北）：101580747

华中地区（包括河南、山西、湖北、湖南、江西、安徽、贵州）：17201450
华东地区（包括上海、浙江、江苏、福建、山东、台湾）：32354930
华西地区（包括陕西、四川、重庆、宁夏、甘肃、青海、新疆、西藏）：54435786
华南地区（广东、广西、海南、云南、香港、澳门）：21576699

2．3个专家博客

51CTO博客：http://winda.blog.51cto.com
CSDN博客：http://blog.csdn.net/lycb_gz
ChinaUnix博客：http://blog.chinaunix.net/uid/10659021.html

3．2个认证微博

新浪微博：weibo.com/winda
腾讯微博：t.qq.com/winda2010

4．视频培训

视频培训课程主页：http://edu.51cto.com/lecturer/user_id-55153.html
视频培训学员QQ群：241903278

鸣谢

本书由王达主编并统稿，经过数十位编委、技术专家夜以继日地工作，一次次地严格审校、修改和完善，这本巨作终于完成，并顺利高质量地出版上市。在此感谢华为技术有限公司各位专家慎密的技术审校和大力支持，感谢人民邮电出版社各位编辑老师，以及各位编委的辛勤工作！以下是参与本书编写和技术审校人员名单。（排名不分先后）

编委人员：何艳辉、周健辉、何江林、卢翠环、李　峰、郑小建、余志坚、曾育文、刘云根、谢桂安、罗广平、朱碧霞、胡海侨、黄丽君、王　爽、陈玉生、蔡学军、李　想、夏　强、刘胜华、罗巧芬
技术审校：陈　昊、李云超、刘立灿、莫　雯、闫建刚、周常青

前　言

经过数月、数十位编写人员的辛勤创作和一次又一次的修改，本书终于完稿了，大家也都从这本书内容的专业性和实用性中感受到巨大的成就感。

本书特色

综合起来，本书具有以下许多非常鲜明的特色：

- 本书是华为网络设备技能学习、培训的指定教材。
- 全国第一本，也是目前唯一的华为路由器配置与管理工具图书。

本书所包括的内容非常全面、系统，从最基础的华为交换机路由器选型与维护，路由器的各种登录方式、BootROM 菜单使用、信息中心管理、U 盘开局配置和自动配置，到主流应用的各种路由器接口、WAN 接入与互联、DHCP/DNS 服务、NAT 等基础功能，再到 BFD/NQA、VRRP、接口备份和双机热备份等可靠性管理功能，以及静态路由、RIP 路由、OSPF 路由、IS-IS 路由、BGP 路由和路由策略/策略路由等各种路由功能配置与管理无一不囊括其中。真正的“一册在手，别无所求”。

- 深入浅出的技术原理剖析与分层次配置示例的完美结合。

本书不仅有比较深入的各种华为路由器技术原理剖析，而且列举了大量各种不同级别的应用配置示例。这种有机结合可以使广大读者朋友，特别是初级读者朋友不再是孤立地去学习枯燥的技术原理，而是能体验到这些技术原理在实际工作中的具体应用，反过来又加深了对这些技术原理的理解。另外，书中大量的配置示例也是分层次的，这样就使读者朋友不仅可以全面了解各具体配置命令的使用方法，更能深入地理解不同配置命令之间的相互关联及灵活应用。

- 综合配置思路分析和详尽配置步骤介绍完美结合。

本书在介绍华为路由器功能配置与管理时，注意配置思路分析与配置步骤介绍的完美结合，而不是机械地罗列出各种功能配置步骤。这样可使读者朋友在“知其然”的同时“知其所以然”，可以充分理解各种具体功能的基本配置和实现原理，可以在实际的网络设备配置工作中做到举一反三，灵活应用。

适用读者对象

本书的内容非常全面、系统，适合于各层次的读者，具体如下：

- 使用华为路由器产品的用户；
- 华为培训合作伙伴以及华为网络学院的学员；
- 高等院校的计算机网络专业学生；
- 希望从零开始学习华为路由器配置与管理的读者；
- 希望能系统学习华为路由器配置与管理的读者；

- 希望有一本可在平时工作中查阅的华为路由器配置手册的读者。

本书介绍的 AR G3 系列路由器目前已广泛应用于政府、金融、能源、交通、电力、教育、电信运营商等行业或企业市场。AR3200 系列企业路由器采用了嵌入式硬件加密，支持语音的数字信号处理器（DSP）插槽、防火墙、呼叫处理、语音信箱以及应用程序服务，支持业界应用最广泛的有线和无线连接技术，如 E1/T1、xDSL、xPON、CPOS、3G、LTE 等，提供包括有线和无线的连接应用方式，如 Internet 接入、专线接入，以及 PBX、融合通信及安全等功能，广泛部署于大中型园区网出口、大中型企业总部或分支等场景。

AR2200/2200-S 系列企业路由器是华为技术有限公司推出的面向中型企业总部或大中型企业分支等以宽带、专线接入、语音和安全场景为主的路由器产品，采用了嵌入式硬件加密，支持语音的数字信号处理器（DSP）插槽、防火墙、呼叫处理、语音信箱以及应用程序服务，支持业界最广泛的有线和无线连接技术，如 E1/T1、xDSL、xPON、CPOS、3G、LTE 等。

AR1200/1200-S 系列企业路由器是华为技术有限公司推出的面向中小型办公室或中小型企业分支的多合一路由器，提供包括有线和无线的 Internet 接入、专线接入，PBX、融合通信及安全等功能，支持语音的数字信号处理器（DSP）、防火墙、呼叫处理、语音信箱以及应用程序服务，支持业界最广泛的有线和无线连接方式，如E1/T1、xDSL、xPON、WLAN、3G、LTE 等。AR1220V、AR1220W/AR1220W-S、AR1220VW 的吉比特固定以太接口还支持 PoE 功能，广泛部署于中小型园区网出口、中小型企业总部或分支等。

AR150/150-S/160/200/200-S 系列路由器作为固定接口的路由器，是面向企业分支及小型企业量身打造的融合路由、交换、语音、安全、无线的一体化企业网关，支持广域网的各种灵活接入方式，单一设备就能满足以太、xDSL、3G、LTE、WLAN 等多种接入需求，灵活地为客户提供各种部署方案，节约运维成本。

本书主要内容

本书是国内图书市场中第一本专门介绍华为路由器配置与管理的工具图书，也是华为 ICT 认证系列培训教材。全书共分三篇、15 章，各篇章的基本内容如下。

第一篇　路由器选型及基本功能配置与管理

第 1 章：全面介绍最新一代 AR G3 各个系列（包括 S150/150-S/S160/200/200-S、AR1200/1200-S、AR2200/2200-S、AR3200 系列）和 NE 系列路由器产品的主要特点、各机型硬件配置和软件功能特性，以及主要应用。

第 2 章：全面介绍 AR G3 系列路由器的各种登录方式（包括本地 Console 口/MiniUSB 口登录、Telnet 登录和 Web 登录）的配置方法，以及 VRP 系统启动配置，BootROM 菜单的使用，信息中心、U 盘开局、自动配置等功能的配置与管理。

第 3 章：全面介绍 AR G3 系列路由器的 LAN 和 WAN 接口（包括 Serial 接口、CE1/PRI 接口、E1-F 接口、CT1/PRI 接口、T1-F 接口、3G Cellular 接口、POS 接口、CPOS 接口、PON 接口、ADSL/VDSL/G.SHDSL 接口等）的配置与管理。

第 4 章：全面介绍 AR G3 系列路由器 DCC、PPP/MP/PPPoE 配置与管理。

第 5 章：全面介绍 DHCP 服务器/客户端、DHCP 中继、DHCP Snooping，DNS 客户

端、DNS Proxy/Relay、DDNS 客户端的工作原理，以及 AR G3 系列路由器中这些功能的配置与管理。

第 6 章：全面介绍 AR G3 系列路由器 Basic NAT、NAPT、Easy IP、NAT Server 和静态 NAT/NAPT 等主要 NAT 类型，以及相关的 NAT ALG、DNS Mapping、NAT 关联 VPN、两次 NAT、NAT 过滤和 NAT 映射技术的工作原理及配置与管理方法。

第二篇：可靠性配置与管理

第 7 章：全面介绍 AR G3 系列路由器 BFD 检测原理、NQA 测试原理及其应用，以及静态 BFD 单跳检测、静态 BFD 多跳检测、静态标识符自协商 BFD、静态 BFD 单臂回声、静态 BFD 与接口/子接口状态联动、ICMP NQA 测试等功能的配置与管理。

第 8 章：全面介绍 VRRP 协议报文结构、VRRP 工作原理，以及 AR G3 系列路由器中 VRRP 基本功能和 VRRP 与接口状态、BFD、NQA、路由联动的配置与管理。

第 9 章：全面介绍接口备份特性、双机热备份实现方式和实现机制，以及 AR G3 系列路由器中主备接口备份、负载分担接口备份、主备接口备份联动和通过 VRRP 实现流量切换的双机热备份等功能的配置与管理。

第三篇：路由配置与管理

第 10 章：全面介绍路由的分类、静态路由的组成和主要特点，以及 AR G3 系列路由器中基本静态路由和静态路由与 BFD、NQA 的联动原理及配置与管理。

第 11 章：全面介绍 RIP 协议的报文格式、各种定时器、路由表的形成、路由更新机制、路由度量机制、网络收敛机制，以及 AR G3 系列路由器中 RIP 基本功能、路由环路防止、路由选路控制、路由信息发布/接入控制、网络性能参数和与 BFD 联动等功能的配置与管理。

第 12 章：全面介绍 OSPF 协议 LSA 类型、区域类型、支持的网络类型、各种报文格式、OSPF 状态机，OSPF 邻接关系的建立流程和路由计算原理，以及 AR G3 系列路由器中 OSPF 基本功能、更新 LSA 的泛洪限制，邻居或邻接的会话参数，支持的网络类型，Stub/Totally Stub/NSSA/Totally NSSA 区域，OSPF 安全功能，路由选择控制，路由信息的发布/接收控制，网络收敛性能控制，与 BFD 联动等功能的配置与管理。

第 13 章：全面介绍 IS-IS 路由器/路由类型、两种地址格式、各种 PDU 报文格式，邻居关系建立、LSP 交互、路由渗透、网络收敛和报文验证原理，以及 AR G3 系列路由 IS-IS 基本功能、路由信息交互控制、路由选路控制、路由收敛性能控制、网络安全性和与 BFD 联动等功能的配置与管理。

第 14 章：全面介绍 BGP AS、BGP 地址族、各种 BGP 报文格式、各种 BGP 路由属性，BGP 路由选路规则，对等体交互原理，与 IGP 交互原理，以及 AR G3 系列路由器中 BGP 基本功能，路由选路和负载分担，简化 IBGP 网络连接，BGP 路由的发布/接收控制，网络收敛性能控制，BGP 安全性，与 BFD 联动等功能的配置与管理。

第 15 章：全面介绍路由策略工作原理、路由过滤器、3 种策略路由，以及在 AR G3 系列路由器中路由策略过程器、路由策略、本地策略路由、接口策略路由的配置与管理。

在阅读本书时，请注意以下几个地方。

- 书中是以华为最新一代 AR G3 系列路由器的配置为主线进行介绍的。
- 为了避免内容重复，与华为交换机相同的功能部分，如 VRP 系统的使用，以太

网接口和链路、STP、VLAN、ARP、ACL、QoS、IP 组播等，本书均没有介绍，请参见已经出版的《华为交换机学习指南》一书。

- 书中的配置代码中，**粗体**字部分是命令本身或关键字选项部分，是不可变的；*斜体*字部分是命令或者关键字参数部分，是可变的。
- 在介绍各种路由器技术及功能配置说明过程中，对于一些需要特别注意的地方均以**粗体**字格式加以强调，以便读者在阅读学习时引起特别注意。
- 在介绍各种功能配置的过程中针对不同 AR G3 系列路由器中相同功能的不同配置方法或参数取值范围做了特别说明，以便读者能全面了解不同系列路由器的不同配置方法和参数取值范围。
- 在介绍各种功能特性时明确列出了各个 AR G3 系列路由器对这些特性的支持情况，以便读者明确了解自己所使用的机型对相应特性的支持情况。

安全声明

设备升级、打补丁的声明

对 AR 路由器进行升级或打补丁操作时，可以通过核对 MD5 哈希值来校验软件的合法性。为避免软件被篡改或替换，防止给用户带来安全风险，建议用户进行此项操作。

密码配置的声明

配置密码时，如果选择明文模式，密码将会以明文的方式保存在配置文件中。该模式有较高的安全风险，所以请尽量选择密文模式。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。

配置密文模式的密码时，请不要用以下字符作为起始和结束。因为以下面字符为起始和结束符的合法密文，即 AR 路由器可以解密的密文，在配置文件中能显示该用户配置的相同密文。

- V200R005C00 之前的版本：不要输入以“%$%$......%$%$”为起始和结束符的密文。
- V200R005C00 版本：不要输入以“%@%@......%@%@”为起始和结束符的密文。
- V200R005C10 版本及之后的版本：不要输入以“%@%@......%@%@”或“@%@%......@%@%”为起始和结束符的密文。

加密算法的声明

目前 AR 路由器采用的加密算法包括 DES、3DES、AES、RSA、SHA1、SHA2、MD5 等，具体采用哪种加密算法请根据场景而定。请优先采用如下建议，否则会造成无法满足您安全防御的要求。

- 对称加密算法建议使用 AES（128 位及以上密钥）。
- 非对称加密算法建议使用 RSA（2048 位及以上密钥）。
- 哈希算法建议使用 SHA2（256 位及以上密钥）。
- HMAC（基于哈希算法的消息验证码）算法建议使用 HMAC-SHA2。

个人数据的声明

您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据，因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

特性使用的声明

- AR 路由器支持通过 FTP、TFTP 及 SFTP 传输文件。使用 FTP、TFTP、SFTP v1 协议存在安全风险，建议您使用 SFTP v2 方式进行文件操作。
- AR 路由器支持通过 Telnet 协议和 STelnet 协议登录。使用 Telnet、STelnet v1 协议存在安全风险，建议您使用 STelnet v2 登录设备。
- AR 路由器支持 HTTP 协议和 HTTPS 协议登录 Web 网管。使用 HTTP 方式存在安全风险，建议您使用 HTTPS 方式登录 Web 网管。
- AR 路由器支持通过 SNMP v1、SNMP v2c 和 SNMP v3。使用 SNMP v1 和 SNMP v2c 存在安全风险，建议您使用 SNMP v3 管理设备。
- AR 路由器支持镜像功能，该功能主要用于网络检测和故障管理，可能涉及使用个人用户某些通信内容。华为公司无法单方采集或存储用户通信内容。建议您只有在所适用法律法规允许的目的和范围内方可启用相应的功能。在使用、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。
- AR 路由器支持 NetStream 功能，该功能主要对网络中的业务流量情况进行统计与分析。在提供业务过程中，可能涉及个人数据使用。因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施，以确保用户的个人数据受到充分的保护。
- AR 路由器支持报文捕获功能，该功能主要用于检测通信传输中的故障和错误。华为公司无法单方采集或存储用户通信内容。建议您只有在所适用法律法规允许的目的和范围内方可启用相应的功能。在采集、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。
- AR 路由器支持入侵防御 IPS、URL 过滤功能，这些功能涉及采集或存储个人用户通信内容。华为公司无法单方采集或存储用户通信内容。建议您只有在所适用法律法规允许的目的和范围内方可启用相应的功能。在使用、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。

命令使用的声明

本书中主要介绍了您在使用华为 AR 路由器进行网络部署及维护时，需要使用的命令。对用于生产、装备、返厂检测维修的接口（命令、接口或者其他），不在本书中说明。

对于部分仅用于工程实施或定位故障的高级命令，如使用不当，将可能导致设备异常或者业务中断，建议有较高权限的工程师使用。若您需要，请向华为公司申请。

第一篇

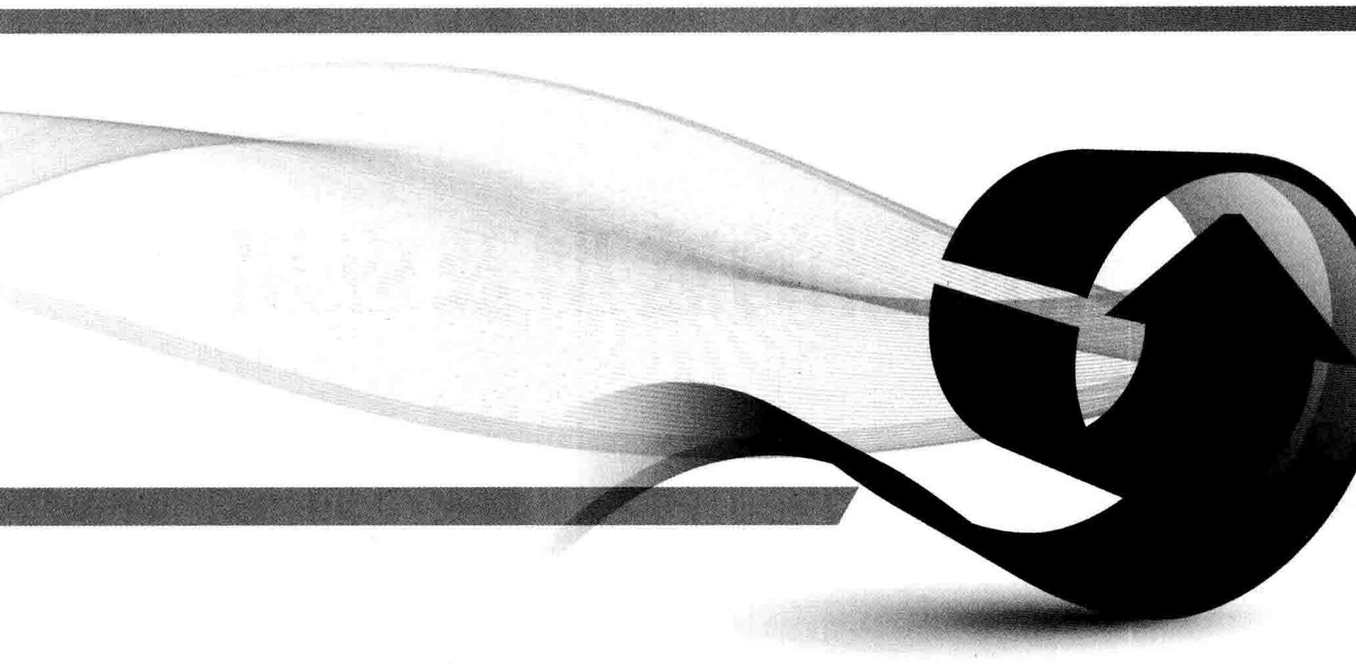
路由器选型及基本功能配置与管理

目　录

第一篇　路由器选型及基本功能配置与管理

第二篇 可靠性配置与管理

第三篇　路由配置与管理



本篇介绍的是华为AR G3系列路由器产品选型和基本功能配置，具体包括以下几章内容。

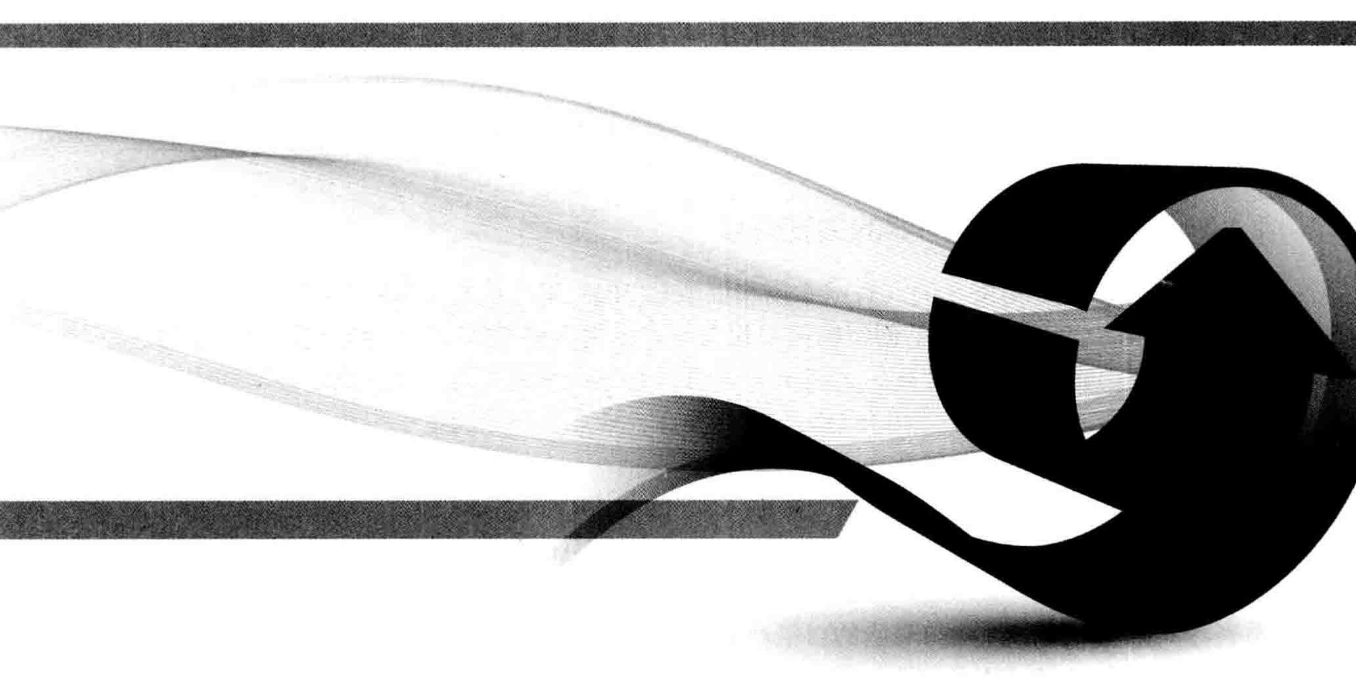
- 第1意　路由器的选型及应用
- 第2章　路由器登录及基础配置
- 第3章　接口配置与管理
- 第4章　WAN接入/互联配置与管理
- 第5章　DHCP/DNS服务配置与管理
- 第6章　NAT配置与管理

本篇介绍的内容都是我们使用AR G3系列路由器产品的前提和基础。在我们进行网络系统设计时，首先要明确的是各种网络设备产品的选型，在确定哪一层要用到哪些功能后就要了解哪个系列的产品可以实现这些功能，它们各自又有哪些机型可供选择，各自的主要特点是什么，这就是第1章的主要内容。

另外，在使用AR G3系列路由器时，我们首先要熟悉路由器产品的VRP系统，以及配置像路由器系统启动与登录、BootRom菜单、信息中心、U盘开局（通过U盘中保存的配置信息自动配置路由器）、Auto-Config（自动配置）等，这就是第2章的主要内容。另外，还必须对各种路由器接口（特别是各种WAN接口），以及WAN接入方式进行配置，这就是第3章和第4章的内容。

本书第5章讲的DHCP和DNS服务配置与管理，以及第6章讲的NAT配置与管理则是路由器应用最广的三种IP服务功能，特别是DHCP和NAT。

第1章
路由器的选型及应用



目前在华为公司的路由器产品中，广泛应用的主要就是两大系列：一个是用于各种规模企业和企业分支网络广域网接入/互联，集路由、交换、语音、安全、有线/无线Internet接入的最新一体化企业网关AR G3系列，一个是面向企业IP网络骨干节点、汇聚节点、边缘节点和数据中心，提供多业务，甚至全业务的汇聚处理，或者大型路由器集群的NE系列。本书以AR G3系列路由器为主线进行各种功能配置介绍。

本章首先重点、全面地介绍广泛应用于各种规模企业或企业分支网络的AR G3系列的主要特点、产品系列、命名规则、主要特性和总体应用，然后依次介绍其中的AR150/150-S160/200/200-S/1200/1200-S/2200/2200-S/3200各个系列的产品特点、主要机型、基本配置规格、产品外观结构、指示灯和主要应用，同时还将对一些功能和应用场景类似的路由器系列，如AR150/150-S/160/200/200-S系列、AR1200/1200-S/2200/2200-S/3200系列进行横向综合比较，以便更好地帮助用户对AR G3路由器产品选型。在本章的最后简单介绍NE大系中的NE20E-S、NE40E和NE5000E三大系列路由器的主要特点和特性。

1.1 华为 AR G3 系列路由器概述

AR G3 系列路由器是华为公司推出的第三代接入路由器，可以为客户提供数据、语音、视频、安全等业务的统一承载，实现灵活、开放、高可靠、易管理的一站式通信解决方案。它所包含的几个子系列以及几十款机型满足了从小型企业，中型企业到大型企业用户几乎所有企业网络接入需求。

1.1.1 AR G3 系列路由器的主要特点

2011 年华为公司发布的（有些系列和机型是 2013 年才正式发布的）第三代企业接入路由器 AR G3 系列采用了创新的第三代架构、采用多核 CPU 及大容量交换网，是集安全、语音、WAN 接入/互联、无线于一体的多业务企业路由器。它提供了移动和固定两类网络接入方式，支持“All In One”多业务合一处理，充分满足了中小企业或大型企业的分支机构的多业务发展新需求。

目前，AR G3 系列企业路由器（简称 AR）包含 AR150、AR150-S、AR160、AR200、AR200-S、AR1200、AR1200-S、AR2200、AR2200-S 和 AR3200 几个系列，其中不带“-S”的是华为公司自销产品系列，带有“-S”的均为华为公司为分销商特别定制的分销产品系列，其整体配置和性能与对应的自销产品系列相当。

综合而言，AR G3 系列路由器具备以下六大方面的鲜明特点。

1. 多核/无阻塞交换

AR G3 系列路由器采用最新的多核处理器架构（最高可支持 12 核），同时，软件系统实现了转发面、业务面和控制面的彻底分离，使其在面对多业务时的处理性能更加从容，流量转发不再有瓶颈，性能较上一代产品提升了 2～3 倍。

【经验之谈】这里所说的“转发面”、“业务面”和“控制面”是路由器体系架构的三个主要功能组成部分。其中“转发面”（也称“数据面”）是决定对流入接口的数据报文进行何种处理，如依据报文中的目的 IP 地址及其他属性参数，根据路由表选择适当的路由路径进行转发；而“业务面”是负责用户业务数据（如 VLAN、VPN，以及像 DHCP、DNS、ICMP 等业务数据）的计算和处理，主要是由路由器 CPU 完成；“控制面”则是用来实现网络拓扑结构的互联，主要是由各种路由协议控制哪条路由将进入对应的协议路由表中，如在路由可达性、路由属性或者所应用的路由发生改变时及时做出相应的路由调整。

总体来说，就是“控制面”负责建立路由路径，“转发面”负责按照“控制面”建立的路由路径转发数据，而“业务面”则是对进入设备的业务数据进行计算和处理。

AR G3 系列路由器还首次采用 160 Gbit/s 大容量交换网，在接口卡与接口卡之间、接口卡与处理器之间有多条网状结构通道，从而可以使数据无阻塞地实现转发，满足多个终端 1 000 Mbit/s 的接入能力。同时，AR G3 系列路由器的总线带宽最高可达 10 Gbit/s，确保了网络处理的性能不再有障碍。

此外，AR G3 系列路由器为了增加系统的可靠性，在板卡热插拔、电源、风扇等关键硬件方面做了充分的冗余设计。考虑到主控板相当于设备的大脑和引擎，AR G3 系列

路由器是首次在企业级中低端路由器上实现了双主控冗余备份，也是业界首款全系列支持板卡热插拔的接入路由器，在企业进行扩容或更换故障板卡时，完全无需中断业务。

2. 集多功能于一身

AR G3 系列路由器除了集成了传统路由器所支持的路由和交换功能外，还提供语音通信和网络安全管理功能。

语音通信是企业的基础业务之一，为此，AR G3 系列路由器不仅内置了 PBX（Private Branch Exchange，专用分支交换）集团电话功能，而且具备多种面向应用的扩展和易用性的设计，如多方通话功能、排队自动接续、彩铃、一号通、话单管理、用户管理等。此外，AR G3 系列路由器还集成了如智能呼叫路由、QoE（Quality of Experience，体验质量）功能实时监测、抖动缓冲、回声消除、丢包补偿等机制和功能，保证语音业务的流畅、清晰和高可用性。选用合适的机型并配置相应的模块，AR G3 路由器可作为企业语音业务网关。

在网络安全管理方面，AR G3 系列企业路由器提供了多种安全接入功能，满足企业分支之间、企业分支与总部之间、合作伙伴访问企业内部信息的需求。如内置了防火墙功能，支持 802.1x 认证、MAC 地址认证和 Portal 认证的端口安全机制，以及基于 Radius 和 HWTACACS 方案等多种 AAA 认证方式；提供了 IPSec VPN、GRE VPN 等安全隧道，实现数据的安全访问与传输，支持分支机构侧隧道的快速部署，隧道认证等功能。从用户接入控制、报文检测到主动防御形成了一套完整的安全防护机制，使得企业用户在顺利开展业务的同时，可以有效地保障企业网络安全。

3. 集成 WLAN AC 功能

对于成长型的企业来说，随着需要部署无线设备的地方越来越多，简单的胖 AP 组网方式因管理复杂、维护困难、安全性差、不能实现无缝漫游和自动升级等弊端，已经不能满足企业发展的新需求；而瘦 AP+AC（接入控制器）的组网方式则很好地解决上述难题，成为了企业部署无线网络的首选。不过单独的 AC 产品价格较高，对于一般企业（尤其是中小企业）来说是个不小的负担。

AR G3 系列路由器也在与时俱进，全系列创新地加入了 AC 功能，还能通过 WEP（Wired Equivalent Privacy，有线等效加密）、WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）、WAPI（WLAN Authentication and Privacy Infrastructure，无线认证和保密基础结构）、802.1x 等安全认证技术，实现通过 WLAN 的业务安全接入，成为了目前国内唯一实现软件支持 AC 功能的企业级路由器产品，为成长型的企业提供了最具性价比的新选择。在这个移动办公和 BYOD（Bring Your Own Devices，自带设备）逐步流行的新时代，选择了 AR G3 路由器，你无需单独购买 AC 设备，也能打造高效、安全、易管理的企业无线网络。

4. 全面广域网接入/互联方式支持

AR G3 系列路由器提供了从光纤、铜缆有线广域网接入/互联接入方式及 Wi-Fi、3G、LTE 无线广域网接入/互联方式的全面支持，能满足多种接入方案的需求。

在 3G 无线接入方式中，AR G3 系列路由器部分机型为当前国内以及全球最主流的 WCDMA、TD-SCDMA 和 CDMA2000 这三大 3G 网络标准提供了全面的支持，满足企业分支机构之间以及与总部间的无线互联需求。用户只需要购买一台设备，就可以随时

使用和更换不同的3G网络，不仅为用户节省了投资成本，也再无后顾之忧。

另外，AR G3系列路由器部分机型还同时支持目前最新的TDD-LTE（时分双工LTE）和FDD-LTE（频分双工LTE）两种LTE（Long Term Evolution，长期演进）4G无线接入方式。

5. 开放业务平台的云体验

AR1200/2200/3200三大系列产品基于开放业务平台（Open Service Platform，OSP）开发，合作伙伴和最终客户都可以按需扩展业务，业务扩展就像超市购物一样简单，可以轻松应对企业千变万化的业务需求。

目前云计算浪潮不断逼近，AR G3系列路由器为了适应发展的趋势，在继承了以往高性能、多业务的同时，专门为云分支推出了云业务增强特性，具备加速云业务效率、提高云业务可靠性、增强云业务扩展性的功能。被业界称为“云时代路由器设备的标杆”。

另外，通过OSP，AR G3系列路由器可以很好地与第三方IT系统集成和对接，为企业客户实现统一通信的业务体验。这使得客户、代理商、第三方和厂家都可以是开发者和使用者，能真正实现业务价值链的共赢，实现快速集成与定制业务，满足用户个性化需求深度融合各类业务，无需部署专门的服务器，节省投资，易于管理与云侧业务实时刷新和同步。

6. 超强的易用性和易管理性

在家用领域，Web界面已经普及了，但在企业级领域，提供Web界面的简单配置无疑会很好地提升用户的产品的使用便捷度，特别适合缺乏高级IT管理人才的中小型企业。华为公司应时代所需，其AR G3系列路由器全面提供了Web界面配置与管理功能。通过其支持的U盘开局功能，可使用户在开始部署时预先将开局文件存储在U盘中，这样软件工程师不需要到现场进行现场软件调测。硬件工程师安装好硬件，插入U盘并上电启动设备，设备自动完成系统软件加载和升级，简化了用户操作复杂度；设备可在华为企业网管eSight系统的支持下可通过NQA（Network Quality Analyzer，网络质量分析）技术进行链路实时监控，支持流检测NetStream，为网络运维和优化提供简单有效的手段和数据支持。

1.1.2 AR G3的主要路由器系列

华为AR G3系列路由器目前主要包括AR150/150-S、AR160、AR200/200-S、AR1200/1200-S、AR2200/2200-S和AR3200等系列（其中带“-S”的是专门为分销商定制的对应产品系列），共有几十款产品，是华为公司推出的集路由、交换、无线、语音、安全等功能于一体的新一代业务路由网关设备，满足了不同类型用户的不同需求。这些系列，其性能随着系列名中的数字增大而增强，用户定位不同，这在我们进行AR G3路由器系列选型时是首先要考虑的。

AR150/150-S/160/200/200-S这几大系列的用户定位一样（但总体硬件配置和性能依次提升），均是固定接口的盒式路由器，是面向**企业分支机构及小型企业**量身打造的融合路由、交换、语音、安全、无线的一体化企业网关。

从AR1200系列开始，均为模块化结构路由器，相比前面的AR150/150-S/160/200/

200-S 系列来说，不仅硬件配置和性能有了较大提升（采用了更高性能的处理器），而且在功能支持和可扩展性方面更加强大。AR1200/1200-S 系列是面向**中小型办公室或中小型企业分支机构**的多合一路由器，提供包括有线/无线 Internet 接入、专线接入、PBX、融合通信及安全等功能，广泛部署于中小型园区网出口、中小型企业总部或分支等场景。

AR2200/2200-S 系列相比前面的 AR1200/1200-S 系列在性能和功能支持方面又有较大提升，它们同样为模块化结构企业路由器，是面向**中型企业总部或大中型企业分支机构**等以宽带、专线接入、语音和安全场景为主的路由器产品。

AR3200 系列企业路由器是华为最新推出的 AR G3 系列产品，秉承了华为在数据通信、无线通信、PON（Passive Optical Network，无源光网络）接入及软交换领域的深厚积累，并依托于自主知识产权的 VRP 平台，提供包括有线/无线 Internet 接入、专线接入、PBX、融合通信及安全等功能，广泛部署于**大中型园区网出口、大中型企业总部或分支机构**等场景。

这些系列中包含的机型及各自主要配置和支持的主要特性，将在本章后面具体介绍。

1.1.3　AR G3 系列路由器的命名规则

每一个 AR G3 路由器系列中都包括了许多针对不同用户需求定位的具体机型。为了区分它们不同的产品基本特性，在为这些机型命名时也规定了一些命名规则。整个 AR G3 系列路由器的名称结构如图 1-1 所示，如 AR 157 VM、AR 1220 V，其中的各部分解释如表 1-1 所示。

【AR】【B1 B2 B3 B4】【C1】【-D1】

图 1-1　AR G3 系列路由器的名称结构

表 1-1　AR G3 路由器系列产品的命名规则

数字和字母	含义
B1	产品系列代号：从“0”、“1”、“2”、“3”中选取，数字越大，性能越高。当 $B1=0$ 时，表示低端盒式产品，不支持 SIC（智能接口卡）槽位，此时 B1 可省略。如 AR150\160\200 系列中的 B1 等于 0，而 AR1200/2200/3200 系列中的 B1 分别为 1、2、3
B2	• 当 B1 为 0 时，B2 表示硬件平台的差异，从“1”、“2”、“3”中选取，数字越大，性能越高。当前有 1、2 两个系列的产品（如 AR156\168F\206 等型号中的 B2 分别为 1、1、2），其中“1”代表 4 个 LAN 口的硬件平台，“2”代表 8 个 LAN 口的硬件平台，后续还会规划 3 系列的产品 • 当 B1 不为 0 时，目前 B2 固定为 2，表示为模块化路由器，如 AR1200/2200/3200 系列中的 B2 均为 2
B3	• 当 B1 为 0 时，与 B2 组合表示同一平台下的不同主机系列，如“15”代表 4*FE LAN 口主机系列，“16”代表 4*GE LAN 口主机系列，“20”代表 8*FE LAN 口主机系列 • 当 B1 不为 0 时，B3 表示主机最大支持槽位类型和槽位数信息，对于 AR1200 系列，B3 表示所支持的最大 SIC 槽位数，对于 AR2200/3200 系列，B3 表示所支持的最大 XISC 槽位数。如 $B3=0$，则表示为上行接口固化或者槽位数裁减的降成本机型，此时由后面的 B4 来体现固化的上行接口或者槽位数信息，否则 B4 默认为 0

（续表）

数字和字母	含义
B4	• 当B1为0时，B4表示产品固定的上行接口类型，“1”代表FE/GE接口（如AR151、AR151W-P、AR151G-HSPA+7、AR151G-C、AR201），“2”代表E1/SA接口（目前暂没有此类机型），“3”代表xPON接口，“5”代表E1接口，“6”代表ADSL-B/J接口（如AR156、AR206），“7”代表ADSL-A/M接口（如AR157、AR157W、AR157VW、AR157G-HSPA+7、AR207V、AR207VW、AR207V-P、AR207G-HSPA+7），“8”代表G.SHDSL接口（如AR158E、AR158EVW、AR168F、AR208E），“9”代表VDSL2接口（如AR169F） • 当B1和B3都不为0时，B4固定为数字0，如AR1220L、AR2220和AR2240 • 当B1不为0，B3为0时，B4表示设备支持固定接口类型或SIC槽位数量，“1”代表固定接口类型为GE，如AR2201-48FE；“2”代表产品的固定接口类型为E1/SA，如AR2202-48FE；“4”代表4个SIC槽位，如AR2204
C1	由1～4位大写字母构成，表示产品的附加功能，具体如下。 • W：支持WLAN，如AR151W-P、AR157W、AR157VW、AR158EVW、AR201VW-P、AR207VW、AR1220W、AR1220VW、AR151W-P-S和AR1200W-S • V：支持Voice（语音）功能，如AR157VW、AR158EVW、AR201VW-P、AR207V、AR207VW、AR207V-P、AR1220V和AR1220VW • G：支持3G通信，如AR151G-C、AR151G-HSPA+7、AR157G-HSPA+7和AR207G-HSPA+7 • L：简化版，如AR1220L、AR2220L • E：Enhance，表示支持上行接口增强，支持双上行，或者2线对或4线对的G.SHDSL，如AR158E、AR158EVW和AR208E • F：Fiber，支持GE Combo接口上行
D1	表示产品功能差异，具体如下。 • A：AC（交流供电，缺省配置，可以省略） • D：DC（直流供电），如AR1220D、AR2220D、AR2220LD • 48FE：固定的48个百兆交换接口，如AR2201-48FE、AR2202-48FE • HSPA+7：WCDMA制式，如AR151G-HSPA+7、AR157G-HSPA+7、AR207G-HSPA+7 • C：支持CDMA2000制式，如AR151G-C • P：Power over Ethernet，支持PoE功能，如AR151W-P、AR207V-P

【经验之谈】以上命名规则对于我们进行AR G3系列路由器的选型非常重要，特别是从B4的数字可以看出各机型所支持的上行接口类型(代表了所支持的上行接入方式)，从C1中我们又可得知只有包含有“W”字母的机型才支持WLAN，只有包含“V”字母的机型才支持语音通信，只有包含“G”字母的机型才支持3G无线接入，包含“D”字母的机型才支持直流供电，包含“P”字母的机型才支持PoE供电功能……这样我们就无需一个个机型去核对其所支持的产品特性，可以直接从机型名称中选择所需的机型。

但是，以上命名规则中部分功能（如语音、PoE供电等）对于AR2200和AR3200系列并不是完全适合，因为这些系列是模块化结构，支持多种单板，用户可根据需要选择相应的单板插入对应的槽位中。各系列、各机型的具体特性支持可参见下节的表1-2。

1.1.4 AR G3系列路由器的主要特性

前面说了，AR G3是集路由、交换、WAN接入/互联、无线、语音和安全等功能于一身的多业务合一处理的企业级路由器，所以它所支持的特性非常广泛。当然不同系列，或不同机型在具体特性的支持上会有所差异，各有侧重，具体如表1-2所示，这也是我

们在进行 AR G3 路由器产品选型时的重要参考依据。

表 1-2　AR G3 系列路由器主要特性

特性	子特性	描述	特性支持差异
局域网接入（仅针对路由器中的 LAN 接口，具体参见《华为交换机学习指南》）	VLAN	提供基本 VLAN、Super VLAN、MUX VLAN、Voice VLAN 和 Guest VLAN 的 VLAN 业务；提供通过 GVRP 完成动态 VLAN 的学习功能	仅 AR2204、AR2220、AR2220L、AR2240、AR3200、AR2204-S、AR2220-S 和 AR2240-S 支持 MUX VLAN 特性
	MAC	提供动态 MAC 地址学习和静态 MAC 地址功能；提供 MAC 限制、黑洞 MAC、Sticky MAC 和 MAC 防漂移功能	无
	STP（生成树协议）	提供 STP、RSTP 和 MSTP 功能；提供 STP 安全功能	无
	SEP（Smart Ethernet Protection，智能以太网保护）	提供以太网链路层的环网保护功能，支持开放环、封闭环、单环及多环拓扑，并满足各种拓扑的冗余保护	无
	链路聚合	提供静态端口聚合和基于 LACP 的聚合功能	无
	LLDP（Link Layer Discovery Protocol，链路层发现协议）	提供通过 LLDP 动态发现邻居设备的功能	无
	WLAN	提供无线用户接入功能，无线用户可以访问传统局域网；提供集成 AC 功能	仅 AR151W-P、AR157W、AR157VW、AR158EVW、AR201VW-P、AR207VW、AR1220W、AR1220VW、AR151W-P-S 和 AR1200W-S 支持 WLAN-FAT AP 特性
广域网互联（仅针对路由器上的 WAN 接口）	WAN 接口	提供 FE/GE、同异步串口、Async、CE1/CT1 PRI、E3、E1T1-F、3G/LTEcellular、ISDN BRI、POS（Packet over SONET/SDH，SONET/SDH 上的分组）、CPOS（Channelized POS，通道化 POS）、ADSL、VDSL、G.SHDSL、E1-IMA 和 xPON 等多种上行接口	WAN 接口的支持情况与设备的型号以及安装的单板有关，请以设备的实际情况为准
	链路层协议	提供 PPP/MLPPP（Multilink-PPP，多链路 PPP）、FR/MFR、HDLC、ATM 等链路层协议以及链路协议规定的 OAM 机制；提供 Multi Chassis MLPP、PPP 压缩功能；提供 FR 压缩、FR over IP 功能；提供 PPPoE IPv4 或者 IPv6 接入功能和 PPPoE 拨号功能	AR150、AR160、AR200、AR150-S 和 AR200-S 系列不支持 FR/MFR 和 HDLC
	拨号互联	提供 DCC 拨号机制，并创建逻辑接口承载拨号链路上的业务	无

（续表）

特性	子特性	描述	特性支持差异
广域网互联（仅针对路由器上的 WAN 接口）	PON	提供 EPON（以太网 PON）和 GPON（吉比特位 PON）两种工作模式，实现与 OLT（Optical Line Terminal，光纤线路终端）的对接	AR150、AR160、AR200 和 AR150-S 和 AR200-S 系列不支持 PON 特性
	网桥	提供从用户以太接口到 WAN 网络接口的桥接机制	无
	终端接入	支持 HDLC over TCP 功能	无
	3G/LTE	提供 3G/LTE 上行功能，支持 3G/LTE 数据卡和 3G/LTE SIC 卡两种硬件。用户可以通过 DCC 拨号接入 3G/LTE 网络。支持多 VPN 应用	无
IP 应用	ARP	提供以太的 IP 解析服务	无
	IPv4/IPv6 主机	提供 IPv4/IPv6 地址管理、TCP/UDP Socket 服务、ICMP 协议、Ping/Tracert 工具以及 UDP Helper 等功能服务	无
	IP FRR	支持 IP FRR 功能	无
	IPv6 过渡技术	支持 IPv6 over IPv4 隧道、IPv4 over IPv6 隧道	无
	PBR	提供 IP 单播策略路由（IPv4/IPv6），包括本地策略路由、接口策略路由和智能策略路由（SPR）	无
	DNS	提供域名解析服务，包括 IPv4/IPv6 DNS Client/DNS Proxy 和 IPv4 DDNS Client 服务	无
	DHCP	提供 DHCP 的动态地址服务，包括 DHCP Client（IPv4/IPv6）、DHCP Relay（IPv4/IPv6）、DHCP Server（IPv4/IPv6）功能，同时对 DHCP 服务进行安全控制	无
	NAT	提供地址转换服务，包括 NAT、PAT、PAM（Port Application Mapping）、EASY NAT 和 NAT Server 功能，为各种应用层提供 ALG 转换	无
IP 路由	IPv4 和 IPv6 静态路由	基础路由功能	无
	RIP 和 RIPng	基础路由协议	无
	OSPFv2 和 OSPFv3	基础路由协议	无
	ISIS 和 ISISv6	基础路由协议	无
	BGP 和 BGP4+	基础路由协议	无
	路由策略	基础路由策略功能	无
组播（参见《华为交换机学习指南》）	IGMP（网站控制消息协议）	提供 IGMP 基本功能、IGMP Snooping、IGMP Proxy 功能	仅 AR2200、AR3200 和 AR2200-S 系列支持 IGMP Snooping 功能

（续表）

特性	子特性	描述	特性支持差异
组播（参见《华为交换机学习指南》）	MLD（组播侦听者发现）	提供 MLD 基本功能和 MLD Snooping 功能	仅 AR2200、AR3200 和 AR2200-S 系列支持 MLD Snooping 功能
	组播路由	提供基础的组播路由管理、组播路由的负载分担和 SSM Mapping 功能	无
	PIM（协议无关组播）	提供 IPv4/IPv6PIM-DM/PIM-SM/PIM SSM 功能	无
	MSDP（组播源发现协议）	提供跨域（PIM-SM 域）组播的组播路由功能	无
QoS（参见《华为交换机学习指南》）	MQC（模块化 QoS 命令行）	提供模块化的流量分类策略	无
	优先级映射	提供 LP、802.1P、DSCP 和 EXP 优先级之间的映射	无
	流量监管	提供基于流分类、PVC/VLAN/DLCI、端口的单速双桶和双速双桶算法监管策略	无
	流量整形	提供基于流分类、PVC/VLAN/DLCI、端口的流量整形，支持自适应整形，并提供 HQoS 的三级队列整形	无
	拥塞管理	提供基于流分类、PVC/VLAN/DLCI、端口的三级 HQoS 拥塞管理策略；提供 PQ、WRR、DRR、WFQ、PQ+WRR/PQ+DRR/PQ+WFQ、CBQ 队列机制	无
	拥塞避免	提供基于优先级的 WRED 丢弃和尾部丢弃（Tail Drop）策略的报文拥塞管理机制	无
	HQoS（分级 QoS）	提供基于多级队列的层次化调度，不仅区分了业务，也区分了用户	无
	SAC（智能应用控制）	提供基于 SAC 的流分类器，对报文中的第 4～7 层内容和一些动态协议（如 HTTP、FTP、RTP）进行检测和识别，根据分类结果实施精细化 QoS 策略控制	无
安全（部分参见《华为交换机学习指南》）	AAA	提供管理员用户和接入用户的认证、计费和授权功能，包括本地、RADIUS 和 TACACS 的认证、计费和授权	无
	防火墙	提供基于安全区域的 DMZ 防火墙、包过滤防火墙和应用状态防火墙；提供用户的黑白名单和攻击检测功能	无
	流量抑制	提供基于端口的流量抑制	无

（续表）

特性	子特性	描述	特性支持差异
安全（部分参见《华为交换机学习指南》）	接入安全	提供基于用户和端口的 802.1x 认证、MAC 认证、MAC 旁路认证和 MAC 直接认证功能；提供对于访客用户的 Web 网页的认证和 Guest VLAN 功能	无
	本机防攻击	提供对设备的保护，包括 CPU 防攻击和攻击溯源功能	无
	ARP 安全	提供 ARP 报文抑制、防 ARP 地址欺骗、ARP 网关冲突检查和动态 ARP 检查（DAI）功能	仅 AR2200、AR3200 和 AR2200-S 系列支持 DAI 功能
	IP 安全	提供 IP 层的安全功能，包括 ICMP 防攻击、URPF、IP Source Guard 和 DHCP Snooping 功能	仅 AR2200、AR3200 和 AR2200-S 支持 IP Source Guard 和 DHCP Snooping 功能
	PKI	提供证书申请、更新和验证功能	无
	HTTPS	提供 HTTPS 服务器功能，利用 SSL 协议的数据加密，身份验证等特性，可以保证用户和设备之间传输的安全性	无
	ACL	提供基于物理端口、二层信息、IP 协议和 TCP/UDP 端口的流量分类功能	无
可靠性	接口备份	提供各种广域网接口相互备份机制，保证业务的可靠性；支持接口备份与 NQA 联动、接口备份与 BFD 联动、接口备份与路由联动	无
	VRRP	为 IP 服务提供一个冗余选择备份的机制，包括 IPv4/IPv6 VRRP	无
	BFD（双向转发检测）	支持单跳和多跳 BFD，支持 BFD for VRRP、BFD for 路由协议	无
	ETHOAM（以太网操作、维护与管理）	提供 IEEE 802.3ah 实现点到点以太网故障管理	无
设备管理	信息中心监控设备	提供单板管理、电源管理、风扇管理、电子标签的信息监控功能	无
	版本管理	提供在线版本升级、回退、补丁加载功能	无
	镜像监控设备	提供基于端口和基于流分类的镜像功能	无
	远程 PoE 供电	提供基于 LAN 侧的以太远程供电功能	仅 AR151W-P、AR201VW-P、AR207V-P、AR1220V、AR1220W、AR1220VW、AR151W-P-S 和 AR1220W-S 支持 PoE 特性
	Web 网管	提供内置 Web 网管功能	无

（续表）

特性	子特性	描述	特性支持差异
设备管理	开局部署	提供基于 USB 自动开局功能；提供整个网络的 Auto-Config（自动配置）功能	无
网络管理	SNMP	提供 SNMP 代理、FM（Fault Management，故障管理）和 TSC（告警开关控制）功能	无
	Ping 和 Tracert	提供网络连通性检测功能	无
	NTP	支持 NTP IPv4/IPv6，提供传统的 IP 网络时间同步功能	无
	RMON	通过 RMON 和 RMON2 实现对某一网段的状况进行监控、流量统计	无
	CWMP	提供基于 CWMP 的设备管理功能，实现对 AR 的远程集中管理	无
	NetStream	提供流量的条件采样和统计功能，所输出的流统计报文格式支持 V5、V8、V9 和 V10	无
	NQA	提供检测网络上运行各种协议性能的功能	无
	IP Accounting	提供信息统计功能，包括： ● 对所有经过设备的 IPv4 数据流进行信息统计 ● 对用户指定的 IPv4 数据流进行信息统计 ● 对所有经过设备的 IPv4 数据流按照 IP 报文优先级进行分类统计	无
MPLS	MPLS 基本功能	提供静态 LSP、PHP（Penultimate Hop Popping，倒数第二跳弹出）功能；提供 MPLS LSP 的 QoS 功能	AR150、AR150-S、AR200、AR200-S 、AR1200-S 和 AR2200-S 系列不支持 MPLS 特性
	MPLS LDP	提供 MPLS LDP 功能	
	MPLS TE	提供 MPLS TE 功能	
	MPLS FRR	提供 LDP FRR、TE FRR、VPN FRR 功能	
	MPLS over GRE	提供 MPLS LDP over GRE、L2VPN over GRE、L3VPN over GRE 功能	
	6VPE（IPv6 提供商 VLN 边缘）	提供 IPv6 over MPLS 功能	
VPN	IPSec VPN	支持基于 IKE V1/V2 协商的 IPSec 隧道，提供分支和总部的互联功能；提供基于硬件加速的 MD5 和 SHA 的认证算法；提供 AES、DES、3DES 加解密算法	无
	SSL VPN	提供虚拟网关和 SSL VPN 前置功能，管理 SSL VPN 用户和 SSL VPN 业务	无

（续表）

特性	子特性	描述	特性支持差异
VPN	DSVPN（动态智能 VPN）	提供 DSVPN 功能，在分支和分支之间通过 NHRP，动态建立数据转发通道	无
	L2TP（二层隧道协议）	可以作为 LAC 及 LNS，支持多路用户同时呼入	无
	L3VPN（三层 VPN）	提供基于 BGP 的 L3VPN 互联功能	无
	GRE VPN	提供 GRE 隧道功能，提供分支和总部的互联功能；与 IPSec 结合使用，弥补 IPSec 不能保护组播数据的缺陷	无
语音	线路配置	提供 FXS、FXO、CE1、PRI、BRI 的线路接入和配置	仅 AR157VW、AR158EVW、AR201VW-P、AR207V、AR207VW、AR207V-P、AR1220V、AR1220VW、AR2204、AR2220、AR2220L、AR2240AR2204-S、AR2220-S、AR2240-S 机型和 AR3200 系列支持语音特性
	SIP AG	由软交换等上级设备完成呼叫的控制和管理，与软交换之间的交换通过 SIP 进行；提供本地存活 BEST 功能；提供 SIP over TLS 功能	
	H.248AG	由软交换等上级设备完成呼叫的控制和管理，与软交换之间的交换通过 H.248 协议进行	
	PBX	提供 FXS 的线路接入和配置；支持 SIP 信令；支持呼叫等待业务	

说明 在这里要特别注意一些主要特性（如 MUX VLAN、WLAN、语音、3G、MPLS 等）的产品支持差异。在进行产品选型时，如需要某一特性时，可先参见表中的对应特性中的产品支持情况，以免错误地进行机型选择。技术在不断发展，特性不断丰富，必要时请获取最新资料。

1.1.5 AR G3 系列路由器的主要应用

AR G3 系列路由器一般位于企业网内部网络与外部网络的连接处，是内部网络与外部网络之间数据流的唯一出入口，能将多种业务部署在同一设备上，极大地降低了企业网络建设的初期投资与长期运维成本。用户可以根据企业用户规模选择不同规格的 AR G3 系列路由器作为出口网关设备。

本节全面介绍 AR G3 系列路由器在 WAN 接入/互联、语音、VPN、无线等几个方面的应用（至于具体机型是否支持对应的应用，请参见 1.1.4 小节中表 1-2 的说明），在本章后面还将介绍各主要系列的具体应用。

1．广域网接入/互联

根据运营商提供的网络环境，AR G3 系列路由器的用户可以通过 FE/GE、同异步串口、Async、CE1/CT1 PRI、E1T1-F、3G cellular、ISDN BRI、POS、CPOS、ADSL、VDSL、G.SHDSL、E1-IMA 或者 xPON 接口（这些 WAN 接口的具体配置将在本书第 3 章中介绍）接入 WAN 网络。AR G3 路由器可以提供双上行链路，实现主备接口备份，保证上网业

务的可靠性。各 AR G3 系列路由器的 WAN 接口支持情况与设备的型号以及安装的单板有关，请以设备的实际情况为准。

如图 1-2 所示，企业 A 采用 AR G3 路由器的 ADSL 方式接入网络，企业 B 采用 FE 和 E1/CE1 双链路接入网络（E1/CE1 作为 FE 的备份链路），企业 C 采用 G.SHDSL 方式接入网络，企业 D 采用 3G 方式接入网络。

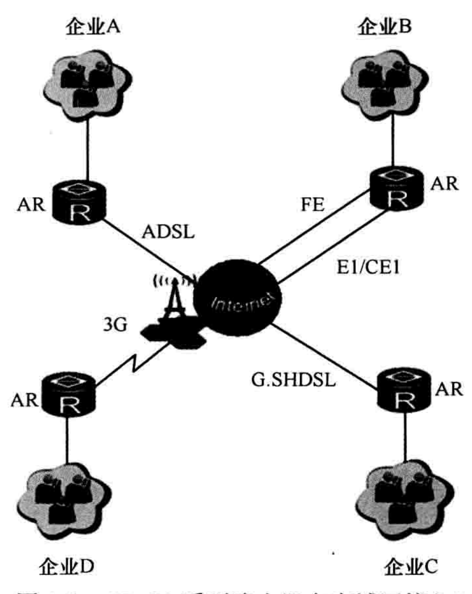


图 1-2　AR G3 系列路由器在广域网接入/互联中的应用

2. VPN 接入

总公司和分支机构可利用 AR G3 系列路由器通过 Internet 互联构建 VPN，以保证数据传输的安全。如图 1-3 所示，公司总部网络通过 AR2200-S 与外部网（Internet）相连，公司分支机构的局域网通过 AR200-S/1200-S 与外部网相连。总部与分支机构、总部与出差人员之间分别建立 GRE/IPSec VPN 隧道和 L2TP/SSL/IPSec VPN 隧道来保证数据的安全传输。公司分支机构和总部建立 VPN 隧道后，分支机构之间可以通过总部进行通信；也可以通过部署 DSVPN，实现分支机构之间动态建立隧道，提升了转发性能和效率，减少了总部的资源消耗。

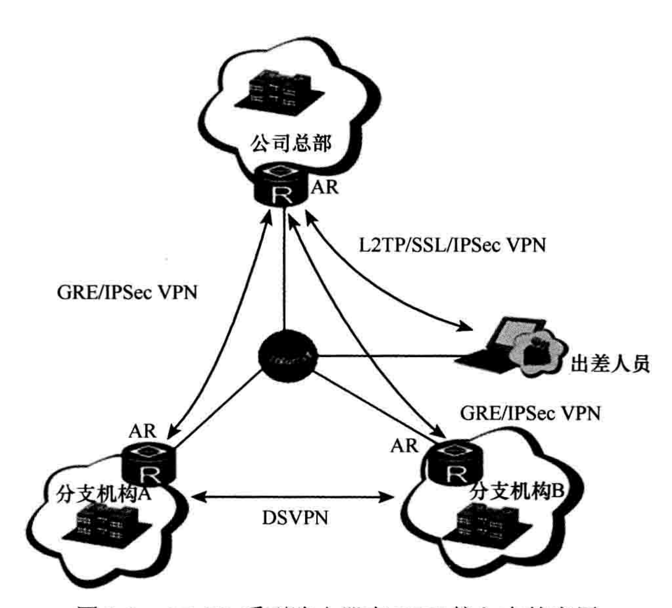


图 1-3　AR G3 系列路由器在 VPN 接入中的应用

3. WLAN 接入

AR G3 系列企业路由器中的部分机型（参见表 1-2）还集成了 WLAN 无线接入功能，支持 802.11a/b/g/n 标准通信，同时软件集成 AC（接入控制器），使得部署和管理更便捷。其丰富的无线功能特性，满足用户的无线接入需求，助力企业灵活构建分支网络，如

图 1-4 所示。

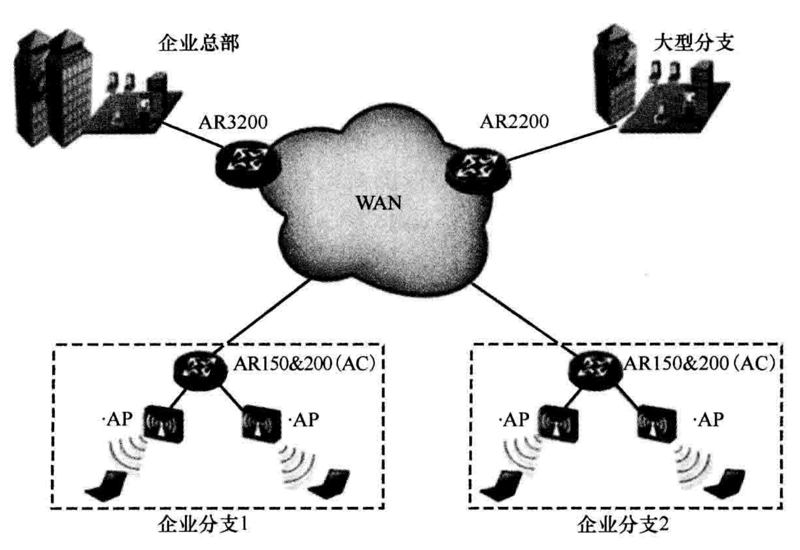


图 1-4 AR G3 系列路由器在 WLAN 接入中的应用

通过集成的 AC 功能，还可对无线局域网中的 AP（接入点）进行控制和管理。AR G3 系列路由器支持丰富的接入认证方式和灵活的用户权限控制，能为 Wi-Fi 用户提供安全接入保证。同时集丰富的无线功能于一身，实现对有线无线一体化网络的集中管理，满足不同规模企业的建网要求。

4. 企业安全保护

AR G3 系列路由器可以部署在企业内部网与外部网的连接处，利用其所支持的各种安全功能保护企业内部网（包括企业内部各局域网）的信息安全。

如图 1-5 所示，企业内部网通过 AR G3 路由器与外部网相连，可以限制外部网用户访问企业内部网，比如禁止外部网用户访问企业的对内服务器，允许访问企业的对外服务器。企业内部的关键部门——财务部、市场部各自组成一个小的局域网。如果企业内部网用户需要访问外部网，可以在进行 NAT 转换之后向外部网发起访问。

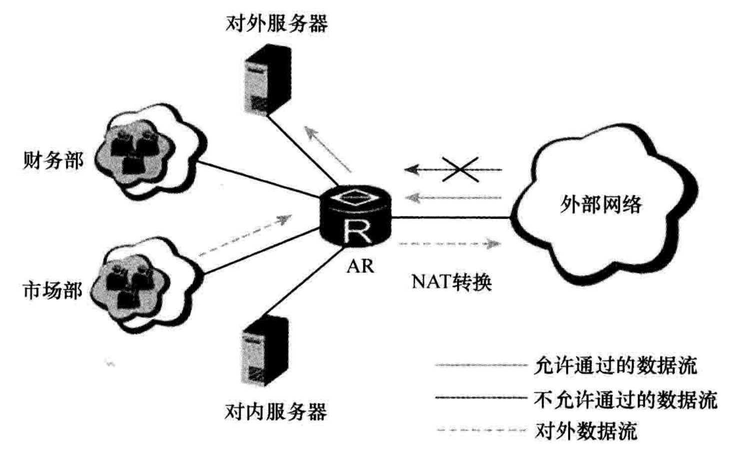


图 1-5 AR G3 系列路由器在网络安全保护中的应用

AR G3 系列路由器可以通过多种方式来保护企业内部网的信息安全。比如：

① AR G3 路由器开启包过滤防火墙或状态防火墙，将企业内部网与外部网进行隔离，保护内部网免受外部非法用户的侵入。

② AR G3 路由器对内网用户提供 NAC（Network Access Control，网络访问控制）机制，针对不同企业员工提供不同的接入权限，保证企业的接入安全。

5. 语音通信

企业基于 IP 网络自建语音通信系统，可以使企业内部的语音通信不产生通信费用，节省企业成本。在搭建语音通信网络时，AR G3 系列路由器可以作为 IP PBX 设备或者 SIP AG（接入网关）设备，下行通过 FXS（外部交换站）接口接入 POTS 用户（模拟电话或传真）、通过 S/T 接口接入 ISDN 电话用户，或者通过以太接口接入 SIPUE 用户（IP 电话或 PC 软终端）。上行可以通过 FXO（外部交换局）或者 E1 接口接入传统 PSTN 网络，或者通过以太接口接入 IP 网络。

如图 1-6 所示，企业分支 A 与企业总部不在同一个号码区域。在企业总部与企业分支都部署 IP PBX（即设备工作在 PBX 形态），作为出口路由器。企业总部的语音用户注册到企业总部的 IP PBX 设备，企业分支的语音用户全部注册到企业分支的 IP PBX 设备，总部与分支之间的语音用户通信通过总部与分支之间的语音路由进行出局，并且总部 IP PBX 为各个分支机构互通提供呼叫路由。

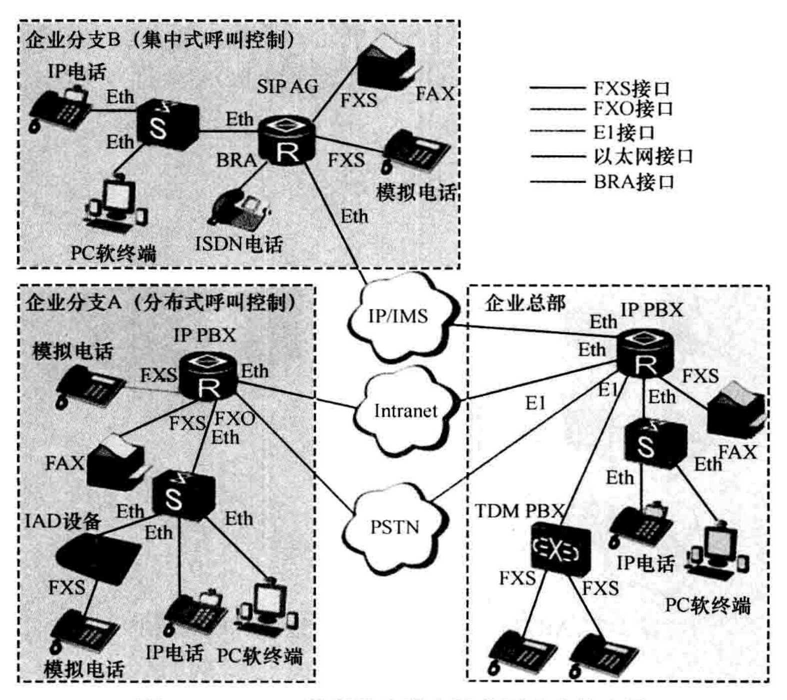


图 1-6　AR G3 系列路由器在语音通信中的应用

企业分支 B 与企业总部之间通过 IP 专网连接，在企业总部部署 IP PBX（即设备工作在 PBX 形态），企业分支部署 SIP AG（即设备工作在 AG 形态）。企业总部与企业分支的语音用户全部注册到企业总部的 IP PBX。总部 IP PBX 为企业内所有用户提供呼叫控制服务。



在 AR G3 系列路由器中并不是所有机型都支持语音通信，具体情况如下。

① AR150 系列中 AR157VW 和 AR158EVW 支持语音功能；AR200 系列中 AR201VW-P、AR207V、AR207VW 和 AR207V-P 支持语音功能；AR1200 系列中 AR1220V 和 AR1220VW 支持语音功能；AR2200 系列中 AR2204、AR2220、AR2220L 和 AR2240 支持语音功能；AR2200 系列和 AR3200 系列如果使用语音功能，建议配置 DSP 模块。

② AR1200 系列、AR2200 系列和 AR3200 系列上需要接入 POTS 用户时，则需购买 4FXS1FXO、16FXS 或者 32FXS 单板。其中，AR1200 系列不支持 32FXS 单板。

③ AR1200 系列、AR2200 系列和 AR3200 系列上需要接入 ISDN 电话用户时，则需购买 2BST 单板。

④ AR150-S、AR200-S 和 AR1200-S 系列不支持语音功能；AR2204-S 和 AR2240-S 支持语音功能，AR2220-S 使用语音功能，建议配置 DSP 模块。

⑤ AR2220-S 需要接入 POTS 用户时，则需购买 4FXS1FXO、16FXS 或者 32FXS 单板。

⑥ AR2220-S 需要接入 ISDN 电话用户时，则需购买 2BST 单板。

6. FTTx 光纤接入

AR G3 系列路由器作为 ONU（光纤网络单元）设备，与 OLT（光纤线路终端）配合实现光纤到企业。如图 1-7 所示，AR G3 路由器通过 PON 上行，实现光纤到家庭、小区和光纤到企业。

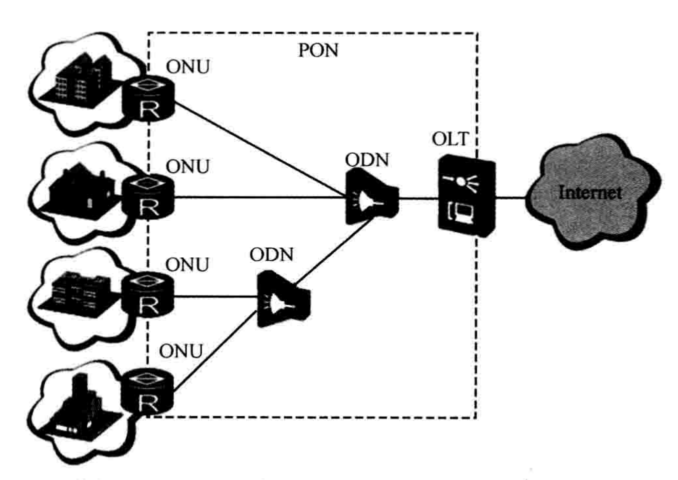


图 1-7 AR G3 系列路由器在 FTTx 接入中的应用

此外，通过 PON 上行实现 FTTx 业务，不仅解决了普通双绞线接入技术带来的带宽不足问题，而且为未来高速率的业务发展提供了保障。

7. OSP 的应用

AR G3 系列路由器提供 OSP（开放业务平台）和统一的软硬件接口，用户可以在此基础上开发出更为丰富的业务。这种开放的业务平台能够让众多不同厂商生产的软件集成在一起。对用户来说，各种自定义的业务可以直接在 AR G3 路由器的 OSP 上安装，

节省了购买服务器的费用，且可以实现统一管理。

如图 1-8 所示，OSP 平台的硬件载体是 SAE（系统架构演进）单板。SAE 单板类似于一台通用 X86 平台的服务器，有独立 CPU、硬盘及内存，还提供外置的 USB 接口、以太网接口、Console 接口和 VGA 显示接口。SAE 单板安装后，由路由器为其供电，对其进行管理和进行数据通信。用户在该单板上安装 VMware，Linux 或者 Windows 操作系统后，可以自行开发或者安装各种第三方的软件应用。

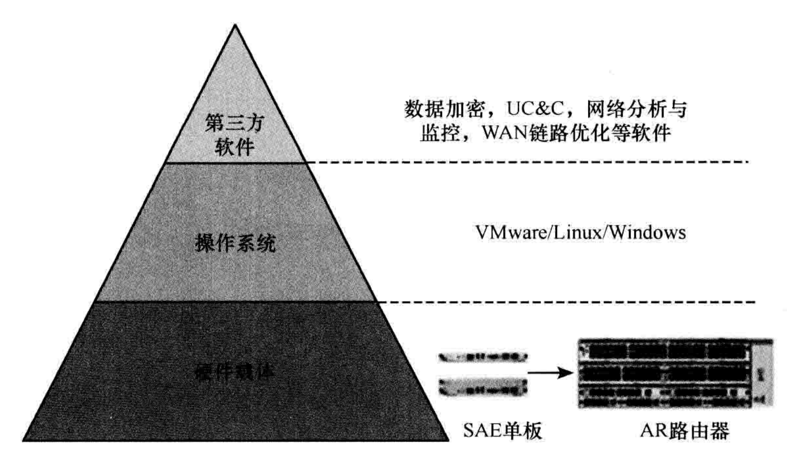


图 1-8　AR G3 OSP 体系结构

说明　SAE 单板有 SAE220（WSIC）和 SAE550（XSIC）两种，不同的设备上可以安装不同数量和形态的 SAE 单板。AR G3 各系列路由器所支持安装的 SAE 单板情况如表 1-3 所示。

表 1-3　　AR G3 系列路由器的 SAE 单板支持情况

设备型号	SAE220	SAE550
AR150-S/200-S 系列	0	0
AR1200-S 系列	1	0
AR2201-48FE-S	0	0
AR2204-S	2	0
AR2220-S	2	1
AR2240-S	4	2

1.2　AR150/150-S/160/200/200-S 系列路由器

之所以把 AR150/150-S/160/200/200-S 这几个系列的路由器放在一起介绍，主要是因为它们的主要用户市场定位基本一样，具有共同的产品特点，都面向企业分支及小型企业量身打造的融合路由、交换、语音、安全、无线的一体化企业网关。它们也都是固定接口路由器，主要差别就在性能和功能的侧重上。

1.2.1 AR150/150-S/160/200/200-S 系列路由器的主要特点

AR150/150-S/160/200/200-S 系列路由器都是固定接口路由器，主要是面向企业分支及中小型企业，是融合路由、交换、语音、安全、无线的一体化企业网关。总体来说，它们具有以下几个方面的主要特点。

1. 高性能

尽管这几个 AR G3 系列路由器都是盒式的固定接口路由器，但由于采用最新一代的体系架构，所以在性能方面仍有相当突出的表现。主要表现在以下几个方面。

① 双倍应用：全系列采用双核处理器，数据转发平面分离，可承载更多的企业应用，并改善数据流叠加时多媒体业务的客户感受。

② 双倍性能：提供领先业界 4 倍的业务处理性能，轻松处理各种企业应用。

③ 双倍潜能：全系列路由器未来可提供向 3G 及 LTE 无线接入的平滑演进方案。

2. 超级实用、易管理

针对这些系列产品主要针对中小型企业用户的特点，华为公司为这些系列产品提供了一系列的实用、易管理的方案。具体表现在以下几个方面。

① 简单构建：真正的即插即用，智能免 IP 配置以及 U 盘开局能力，PPP 和 VPN 指示灯直观显现业务状态，便于快速构建企业 IT 网络。

② 简单方案：提供路由、交换、语音、安全、无线于一体的一揽子解决方案，具有针对特定客户群的快速定制能力，推出契合客户真实需求的解决方案。

③ 简单扩展：全系列 8 端口以太（AR150/150-S/160 系列为 4 端口），可为小型企业提供更多的员工接入能力；灵活可变的双上行 WAN 口，可轻松实现数据负载分担及链路保护，最大程度地保护企业投资。

3. 成熟稳定、安全可靠

虽然是为中小型企业专门设计的，但这些系列产品都是采用华为公司领先的 VRP 操作系统以及 VSP 语音平台，并通过继承性的模块化硬件设计，给企业及分支机构提供成熟、稳定的使用体验。全系列的无风扇设计，提供完美的办公使用体验，并具有恶劣环境适应性，无后顾之忧。

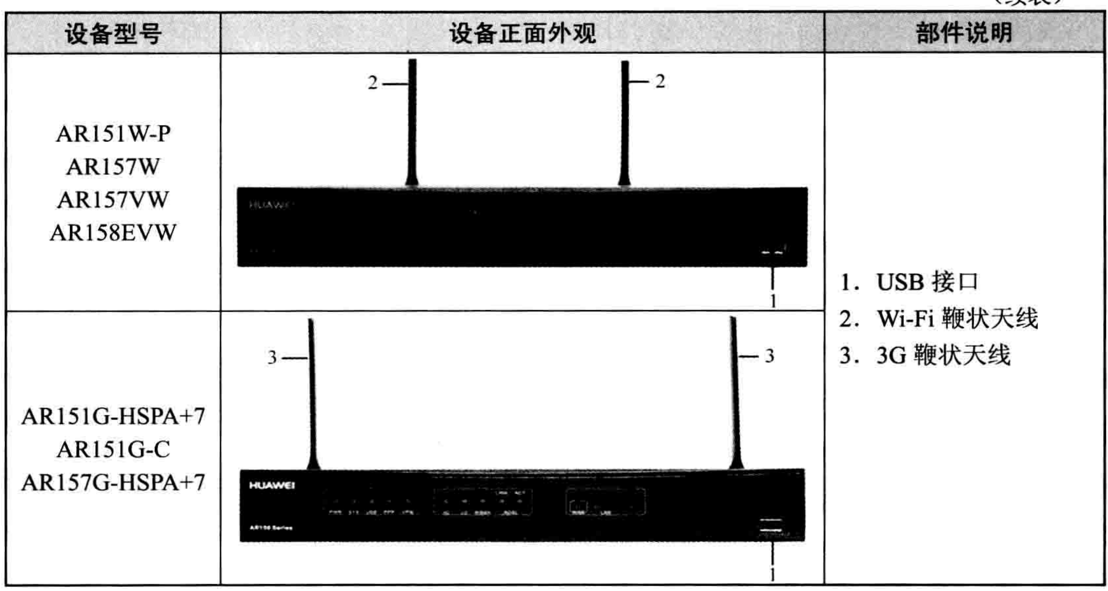
1.2.2 AR150 系列产品外观结构及配置规格

AR150 系列目前共有 11 款产品：AR151、AR151W-P、AR151G-HSPA+7、AR151G-C、AR156、AR157、AR157W、AR157VW、AR157G-HSPA+7、AR158E 和 AR158EVW。这些机型名称中各部分的含义请参照本章前面 1.1.3 小节的介绍，各自的正面外观结构和背面外观结构分别如表 1-4 和表 1-5 所示，各机型的基本配置规格如表 1-6 所示（以官网最新发布为准）。

表 1-4 AR150 系列各设备正面外观结构

设备型号	设备正面外观	部件说明
AR151、AR156 AR157、AR158E	HUAWEI 1	1．USB 接口 2．Wi-Fi 鞭状天线 3．3G 鞭状天线

（续表）

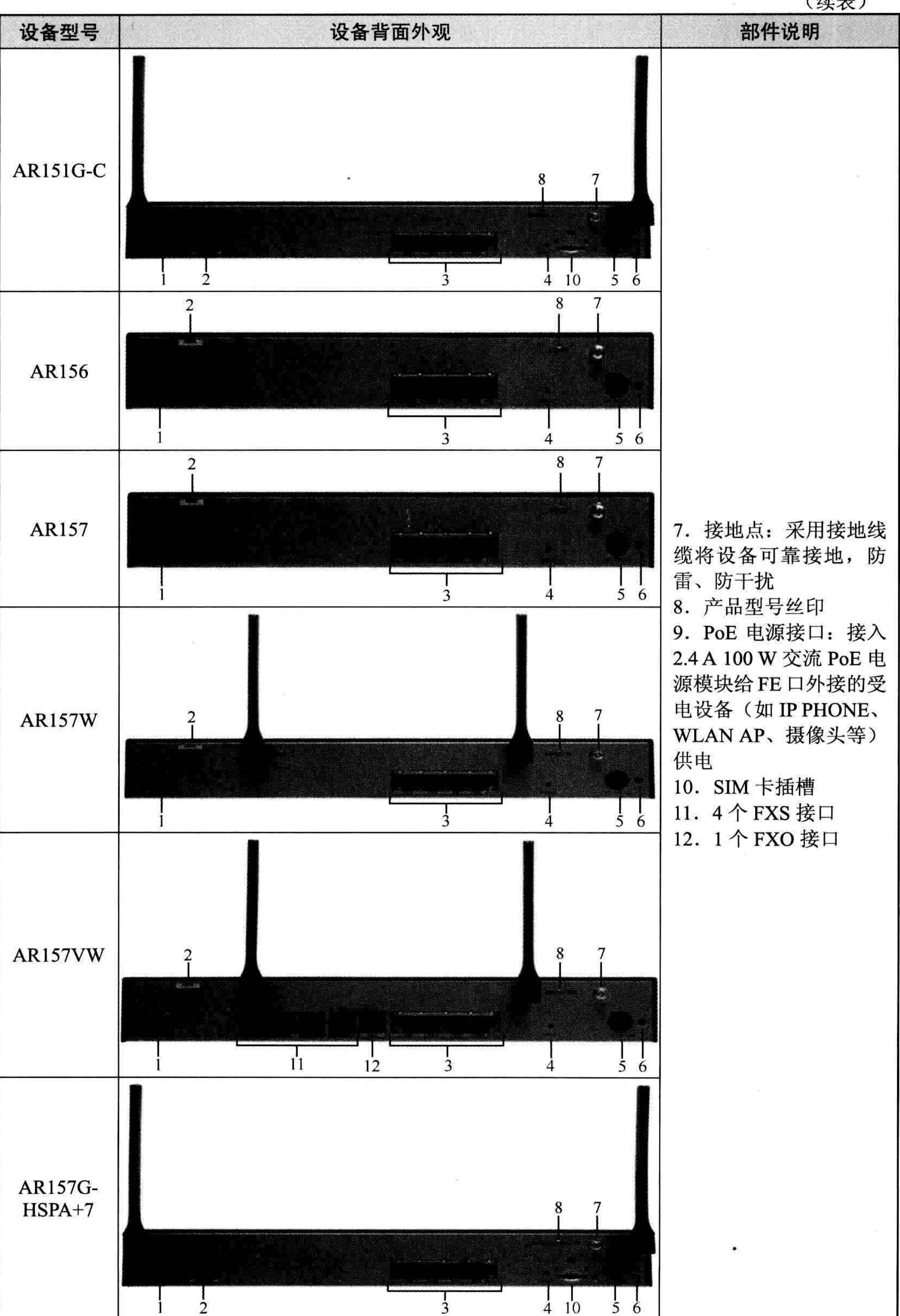


设备型号	设备正面外观	部件说明
AR151W-P AR157W AR157VW AR158EVW		1．USB 接口 2．Wi-Fi 鞭状天线 3．3G 鞭状天线
AR151G-HSPA+7 AR151G-C AR157G-HSPA+7		

表 1-5　　AR150 系列各设备背面外观结构

设备型号	设备背面外观	部件说明
AR151		1. CON/AUX 接口（说明：暂不支持 AUX 功能） 2．WAN 侧接口 • AR151、AR151W-P、AR151G-HSPA+7、AR151G-C：FE 电接口 • AR156：ADSL2+-B/ J 接口 • AR157、AR157W、AR157VW、AR157G-HSPA+7：ADSL2+-A/ M 接口 • AR158E、AR158EVW：G.SHDSL 接口 3．LAN 侧接口 AR150 系列：4 个 FE 电接口 4．RESET（复位按钮，用于手工复位设备，长按（5 s）可恢复出厂配置；短按可复位系统） 5．电源接口：通过接入 2.5 A 24/36/60 W 电源适配器输出 12 V 电压给设备供电 6．电源线扣安装孔：插入电源线扣，用来绑定电源线，防止电源线松脱
AR151W-P		
AR151G-HSPA+7		

（续表）



设备型号	设备背面外观	部件说明
AR151G-C		7．接地点：采用接地线缆将设备可靠接地，防雷、防干扰 8．产品型号丝印 9．PoE 电源接口：接入 2.4 A 100 W 交流 PoE 电源模块给 FE 口外接的受电设备（如 IP PHONE、WLAN AP、摄像头等）供电 10．SIM 卡插槽 11．4 个 FXS 接口 12．1 个 FXO 接口
AR156		
AR157		
AR157W		
AR157VW		
AR157G-HSPA+7		

（续表）

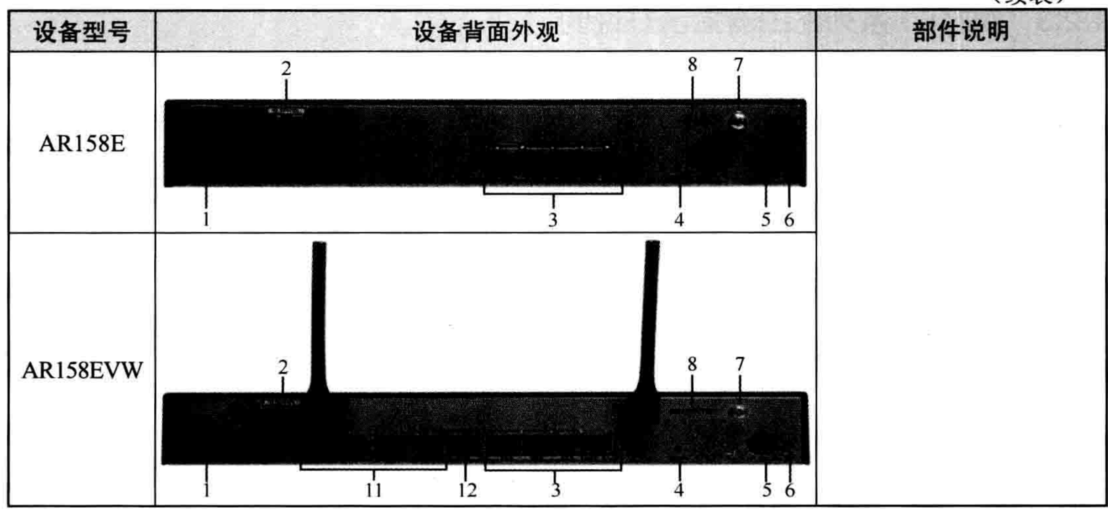
设备型号	设备背面外观	部件说明
AR158E		
AR158EVW		

表 1-6　　**AR150** 系列各机型的基本配置规格

规格名称	AR151	AR151W-P	AR151G-HSPA+7/151G-C	AR156	AR157	AR157W/157VW	AR157G-HSPA+7	AR 158E	AR158 EVW
处理器	双核 533 MHz								
转发性能	300 kpps								
带业务转发性能	100 Mbit/s								
支持的 AP 数（本地转发）	—	4	—			4	—		4
支持的并发用户数（本地转发）	—	80	—			80	—		80
固定 WAN 端口	2×FE（其中 1 个 FE 由以太网交换端口提供）			1×ADSL2+-B/J 1×FE（由以太网交换端口提供）	1×ADSL2+-A/M 1×FE（由以太网交换端口提供）			1×G.SHDSL 1×FE（由以太网交换端口提供）	
固定以太网端口	4×FE								
固定语音接口	—					AR 157VW: 4×FXS+ 1×FXO	—		4×FXS+ 1×FXO
内置 3G	—		WCDMA HSPA+7/ CDMA2000 EVDO	—			WCDMA HSPA+7/ CDMA2000 EVDO	—	
USB2.0 端口	1								
AUX/CON 口	1								
内存容量	512 MB								
Flash 容量	512 MB								
PoE 供电	不支持	支持	不支持						

1.2.3 AR150 系列路由器指示灯说明

AR150 系列路由器指示灯全部在正面板上，但 AR150 系列不同机型的指示灯状态及含义不完全相同，具体如表 1-7 所示。

表 1-7 **AR150** 系列路由器正面板指示灯

机型	指示灯
AR151 AR156 AR157 AR158E	AR151、AR156、AR157 和 AR158E 的指示灯除了 WAN 侧接口指示灯丝印不同外，其他都相同。下图是 AR158E 上的指示灯，各指示灯及状态含义说明如表 1-8 所示 1 2 3 4 5 6 7
AR151W AR151W-P	AR151W-P 的指示灯相对于 AR151W，多 1 个 PoE 指示灯，其他都相同。下图是 AR151W-P 上的指示灯，各指示灯的含义说明如表 1-8 所示 8 1 2 3 4 5 6 9 7
AR151G-HSPA+7 AR151G-C AR157G-HSPA+7	AR151G-HSPA+7、AR151G-C 和 AR157G-HSPA+7 的指示灯除了 WAN 侧接口指示灯丝印不同外，其他都相同。下图是 AR157G-HSPA+7 上的指示灯，各指示灯的含义说明如表 1-8 所示 1 2 3 4 5 10 11 12 6 7
AR157VW AR158EVW	AR157VW 和 AR158EVW 的指示灯除了 WAN 侧接口指示灯丝印不同外，其他都相同。下图是 AR158EVW 上的指示灯，各指示灯的含义说明如表 1-8 所示 1 2 3 4 5 6 9 7 13

表 1-8　AR150 系列路由器的指示灯及状态含义说明

指示灯序号	指示灯/按钮	颜色	指示灯状态含义
1	PWR（电源）	绿色	• 常亮：表明系统供电正常 • 常灭：表明系统无供电
2	SYS（系统）	红绿双色	• 绿色慢闪：表明系统处于正常运行状态 • 绿色快闪：表明系统处于上电加载或者复位启动状态
			红色常亮：表明设备有影响业务且无法自动恢复的故障，需要人工干预
			红灯、绿灯均不亮：表明软件未运行或处于复位状态
3	USB	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，或 USB 接口故障或者指示灯故障
4	PPP	绿色	• 常亮：表明 PPP 业务正常建立 • 常灭：表明 PPP 业务未建立
5	VPN	绿色	• 常亮：表明 VPN 业务正常建立 • 常灭：表明 VPN 业务未建立
6	LINK	绿色	• 常亮：表明 WAN 侧接口链路已经连通 • 常灭：表明 WAN 侧接口链路没有连通
	ACT	绿色	• 闪烁：表明 WAN 侧接口链路有数据收发 • 常灭：表明 WAN 侧接口链路没有数据收发
7	LAN	绿色	常亮：表明该数字对应的 LAN 侧接口链路已经连通
			闪烁：表明该数字对应的 LAN 侧接口链路有数据收发
			常灭：表明该数字对应的 LAN 侧接口链路没有连通
8	PoE	绿色	• 常亮：表明系统 PoE 供电正常 • 常灭：表明系统无 PoE 供电
9	WLAN	绿色	闪烁：表明链路正在传送数据，闪烁的频率随着流量大小而变化
			常灭：表明链路关闭
10	3G	绿色	常亮：表明 3G 信号强
			快闪：表明 3G 信号中等
			慢闪：表明 3G 信号弱
			常灭：表明无 3G 信号
11	2G	绿色	常亮：表明 2G 信号强
			快闪：表明 2G 信号中等
			慢闪：表明 2G 信号弱
			常灭：表明无 2G 信号
12	WWAN	绿色	常亮：表明 3G/2G 处于连接/激活状态
			闪烁：表明 3G/2G 有数据收发
			常灭：表明 3G/2G 处于未连接/未激活状态
13	FXS0～FXS3	绿色	• 常亮：表明该数字对应的 FXS 通道处于呼叫状态 • 常灭：表明该数字对应的 FXS 通道处于空闲状态
	FXO（外部交换局）	绿色	• 常亮：表明该 FXO 通道处于呼叫状态 • 常灭：表明该 FXO 通道处于空闲状态

1.2.4 AR150-S 系列产品外观结构及配置规格

AR150-S 系列是作为 AR150 系列的分销子系列，基本性能与 AR150 系列相当，目前包括以下 3 款产品：AR151-S、AR151W-P-S 和 AR151G-U-S。这些机型名称中各部分的含义请参照本章前面 1.1.3 小节的介绍，各自的正面外观结构和背面外观结构分别如表 1-9 和表 1-10 所示，各自的基本配置规格如表 1-11 所示。

表 1-9　AR150-S 系列各设备正面外观结构

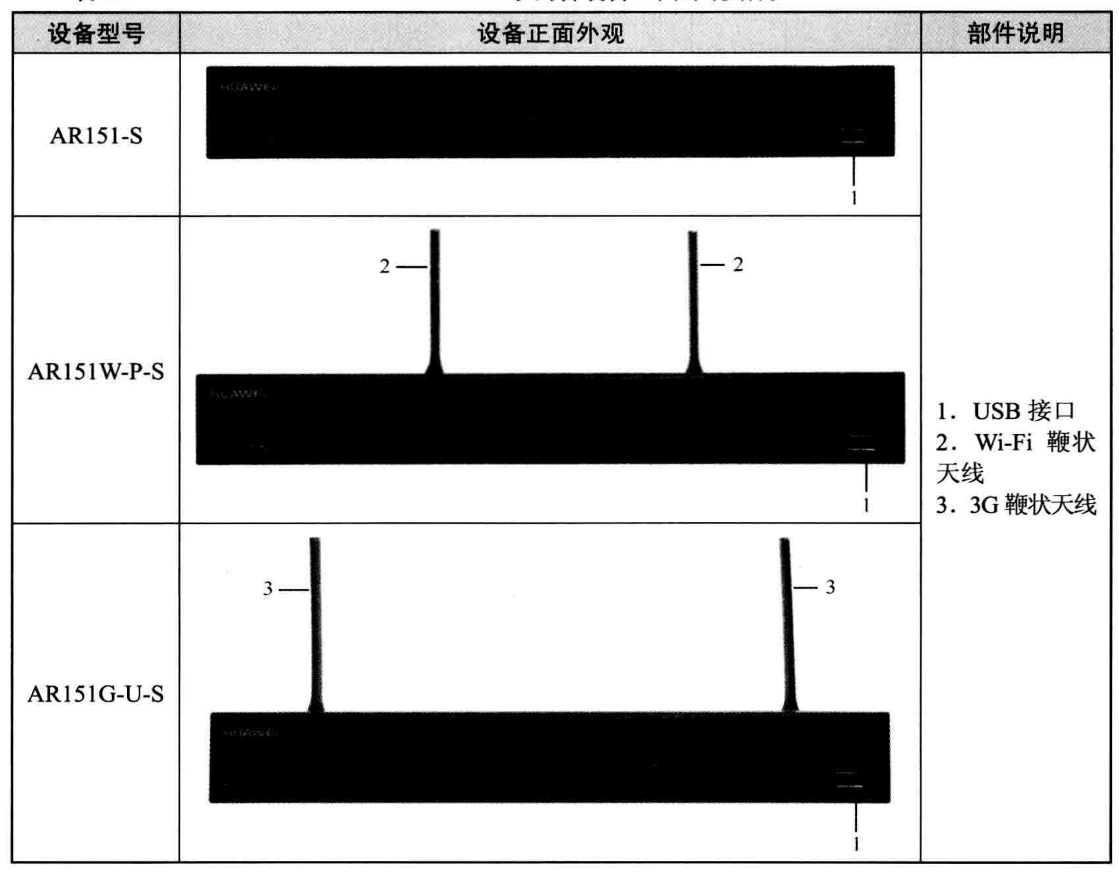
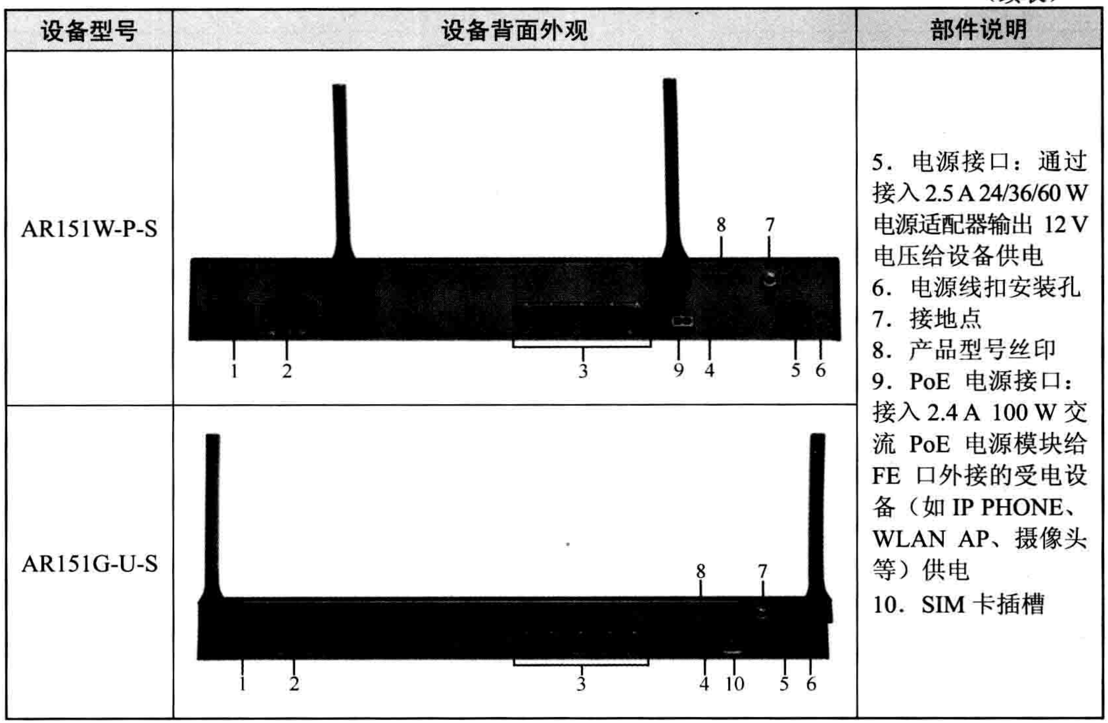
设备型号	设备正面外观	部件说明
AR151-S		1．USB 接口 2．Wi-Fi 鞭状天线 3．3G 鞭状天线
AR151W-P-S		
AR151G-U-S		

表 1-10　AR150-S 系列各设备背面外观结构

设备型号	设备背面外观	部件说明
AR151-S		1．CON/AUX 接口（说明：暂不支持 AUX 功能） 2．WAN 侧接口：FE 电接口 3．LAN 侧接口：4 个 FE 电接口（FE0 接口可以切换成 WAN 口，实现双 WAN 口） 4．RESET

（续表）



设备型号	设备背面外观	部件说明
AR151W-P-S	1 2 3 9 4 5 6 8 7	5．电源接口：通过接入 2.5 A 24/36/60 W 电源适配器输出 12 V 电压给设备供电 6．电源线扣安装孔 7．接地点 8．产品型号丝印 9．PoE 电源接口：接入 2.4 A 100 W 交流 PoE 电源模块给 FE 口外接的受电设备（如 IP PHONE、WLAN AP、摄像头等）供电 10．SIM 卡插槽
AR151G-U-S	1 2 3 4 10 5 6 8 7	

表 1-11　　AR150-S 系列各机型的基本配置规格

规格名称	AR151-S	AR151G-U-S	AR151W-P-S
处理器	双核 533 MHz		
转发性能	300 kpps		
带业务转发性能	100 Mbit/s		
固定 WAN 端口	2×FE（其中 1 个 FE 由以太网交换端口提供）		
固定以太网端口	4×FE		4×FE (PoE)
内置 3G	—	WCDMA HSPA+7	—
USB2.0 端口	1		
AUX/CON 口	1		
内存容量	512 MB		
Flash 容量	512 MB		
PoE 供电	不支持		支持

1.2.5　AR150-S 系列路由器指示灯说明

AR150-S 系列路由器指示灯全部在正面板上，但 AR150-S 系列不同机型的指示灯状态及含义不完全相同，具体如表 1-12 所示。

表 1-12 **AR150-S 系列路由器正面板指示灯**

机型	指示灯
AR151-S	AR151-S 上的指示灯如下图所示，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 1 2 3 4 5 6 7
AR151W-P-S	AR151W-P-S 上的指示灯如下图所示，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 8 1 2 3 4 5 6 9 7
AR151G-U-S	AR151G-U-S 上的指示灯如下图所示，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 1 2 3 4 5 10 11 12 6 7

1.2.6 AR160 系列路由器产品外观及配置规格

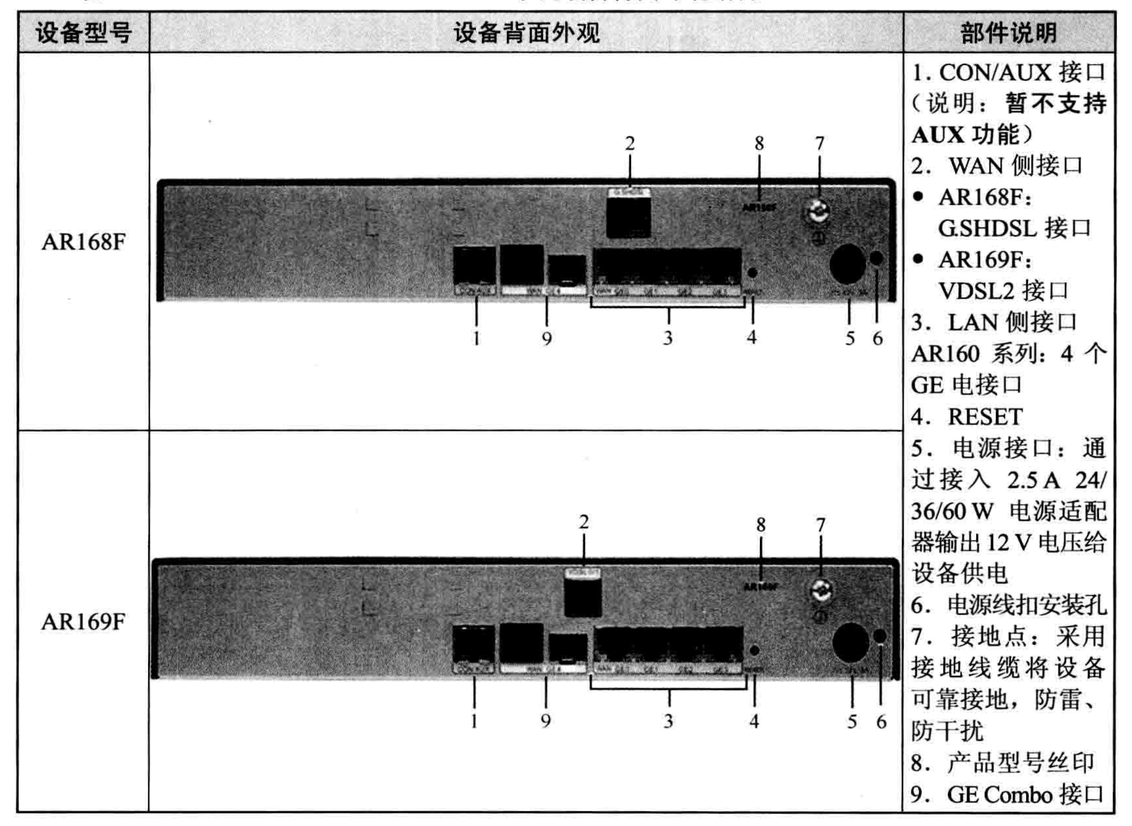
AR160 系列路由器和前面介绍的 AR150/150-S 系列路由器总体差不多，也是面向企业分支及小型企业量身打造的融合路由、交换、安全一体化固定接口企业网关路由器，只是性能有所提升（**转发性能由 AR150/150-S 系列路由器的 300 kpps 提升到 350 kpps，LAN 端口带宽也从 FE 提升到 GE**），而且是专门针对当前最新的 VDSL2 和 G.SHDL 接入方式推出的。

AR160 系列路由器目前仅两款机型，它们是 AR168F（支持 G.SHDL 接入）和 AR169F（支持 VDSL2 接入），**不支持语音通信功能**。它们的正面和背面外观结构分别如表 1-13、表 1-14 所示。AR160 系列路由器的基本配置规格如表 1-15 所示（以官网最新发布为准）。

表 1-13　**AR160 系列设备正面外观结构**

设备型号	设备正面外观
AR168F	HUAWEI USB接口
AR169F	HUAWEI USB接口

表 1-14　**AR160 系列设备背面外观结构**



设备型号	设备背面外观	部件说明
AR168F	2 8 7 1 9 3 4 5 6	1. CON/AUX 接口（说明：**暂不支持 AUX 功能**） 2. WAN 侧接口 • AR168F：GSHDSL 接口 • AR169F：VDSL2 接口 3. LAN 侧接口 AR160 系列：4 个 GE 电接口 4. RESET 5. 电源接口：通过接入 2.5 A 24/36/60 W 电源适配器输出 12 V 电压给设备供电 6. 电源线扣安装孔 7. 接地点：采用接地线缆将设备可靠接地，防雷、防干扰 8. 产品型号丝印 9. GE Combo 接口
AR169F	2 8 7 1 9 3 4 5 6	

表 1-15　**AR160 系列各机型的基本配置规格**

规格名称	AR168F	AR169F
处理器	双核 533 MHz	
转发性能	350 kpps	
带业务转发性能	100 Mbit/s	

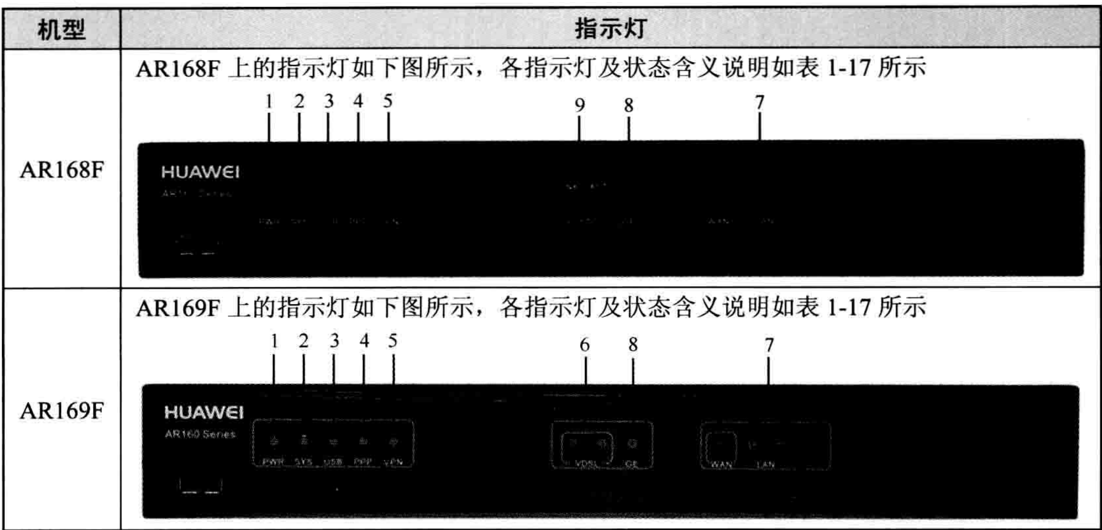
（续表）

固定 WAN 端口	1×G.HSDL、1×FE	1×VDSL2、1×FE
固定以太网端口	4×GE	
USB 端口	1	
AUX/CON 口	1	
内存容量	512 MB	
Flash 容量	512 MB	

1.2.7 AR160 系列路由器指示灯说明

AR160 系列路由器指示灯全部在正面板上，如表 1-16 所示。但两个 AR160 系列机型的指示灯状态及含义不完全相同，具体如表 1-17 所示。

表 1-16　　AR160 系列路由器正面板指示灯



机型	指示灯
AR168F	AR168F 上的指示灯如下图所示，各指示灯及状态含义说明如表 1-17 所示 1 2 3 4 5 9 8 7 HUAWEI
AR169F	AR169F 上的指示灯如下图所示，各指示灯及状态含义说明如表 1-17 所示 1 2 3 4 5 6 8 7 HUAWEI AR160 Series PWR SYS USB PPP VPN VDSL GE WAN LAN

表 1-17　　AR160 系列路由器指示灯及状态含义说明

指示灯序号	指示灯/按钮	颜色	指示灯状态含义
1	PWR	绿色	• 常亮：表明系统供电正常 • 常灭：表明系统无供电
2	SYS	红绿双色	• 绿色慢闪：表明系统处于正常运行状态 • 绿色快闪：表明系统处于上电加载或者复位启动状态
			红色常亮：表明设备有影响业务且无法自动恢复的故障，需要人工干预
			常灭：表明软件未运行或处于复位状态
3	USB	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，或 USB 接口故障或者指示灯故障

（续表）

指示灯序号	指示灯/按钮	颜色	指示灯状态含义
4	PPP	绿色	● 常亮：表明 PPP 业务正常建立 ● 常灭：表明 PPP 业务未建立
5	VPN	绿色	● 常亮：表明 VPN 业务正常建立 ● 常灭：表明 VPN 业务未建立
6	VDSL 左侧指示灯（LINK0）	绿色	● 常亮：表明 WAN 侧接口链路已经连通 ● 闪烁：表明 WAN 侧接口链路正在激活 ● 常灭：表明 WAN 侧接口链路没有连通
	VDSL 右侧指示灯（LINK1）		
7	LAN 侧 4 个 GE 电接口指示灯	绿色	常亮：表明该数字对应的 LAN 侧接口链路已经连通
			闪烁：表明该数字对应的 LAN 侧接口链路有数据收发
			常灭：表明该数字对应的 LAN 侧接口链路没有连通
8	WAN 侧 GE Combo 接口指示灯	绿色	常亮：表明 Combo 接口链路已经连通
			闪烁：表明 Combo 接口链路有数据收发
			常灭：表明 Combo 接口链路没有连通
9	G.SHDSL LINK 指示灯	绿色	常亮：表明 4 路 DSL 通道已全部激活
			1 s 时间内，常亮 0.25 s 时间，剩余 0.75 s 时间内闪烁 3 次：表明 1 路 DSL 通道激活 1 s 时间内，常亮 0.5 s 时间，剩余 0.5 s 时间内闪烁 2 次：表明 2 路 DSL 通道激活 1 s 时间内，常亮 0.75 s 时间，剩余 0.25 s 时间内闪烁 1 次：表明 3 路 DSL 通道激活
			常灭：表明 4 路 DSL 通道均未激活
	G.SHDSL ACT 指示灯	黄色	闪烁：表明有数据收发
			常灭：表明无数据收发

1.2.8　AR200 系列产品外观及配置规格

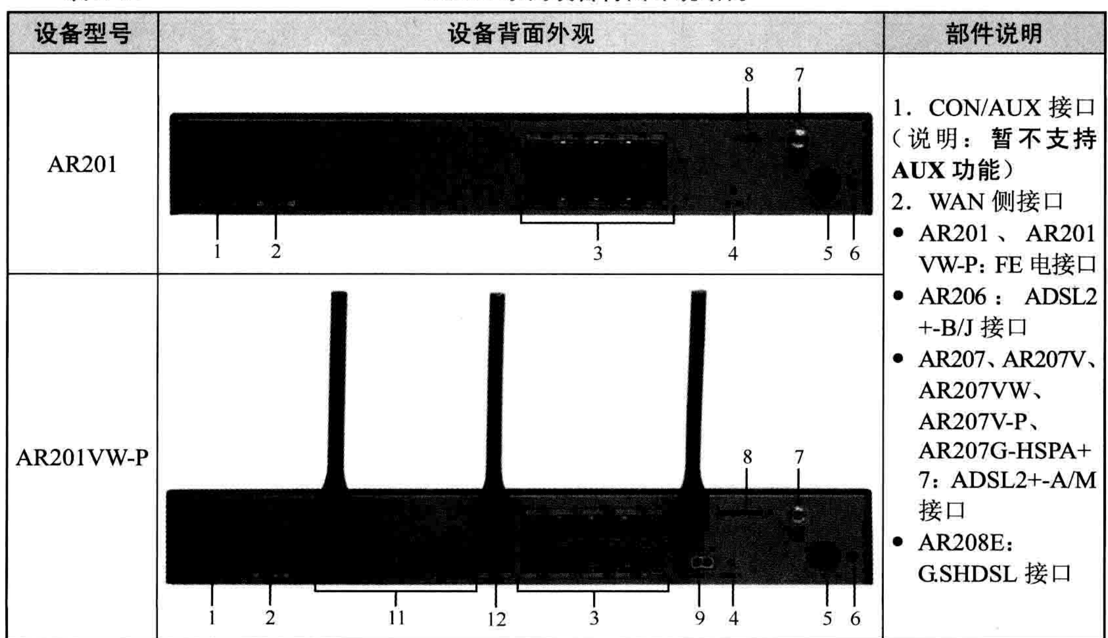
AR200 系列路由器也是固定接口路由器，也是面向企业分支及小型企业量身打造的融合路由、交换、语音、安全、无线的一体化企业网关。与前面介绍的 AR150/150-S/160 系列路由器相比，其转发性能进一步提升，**达到了 450 kpps**（整体性能较 AR150/150-S 系列有近一倍的提升），但其 LAN 口仍与 AR150/150-S 系列一样为 FE 类型，**但扩展到了 8 个 FE 端口**。

AR200 系列路由器目前共有 9 款产品：AR201、AR201VW-P、AR206、AR207、AR207V、AR207VW、AR207V-P、AR207G-HSPA+7 和 AR208E。以上这些产品名称中各部分的含义请参照本章前面 1.1.3 小节的介绍，各自的正面外观结构和背面外观结构分别如表 1-18 和表 1-19 所示，各机型的基本配置规格如表 1-20 所示（以官网最新发布为准）。

表 1-18　　AR200 系列设备正面外观结构

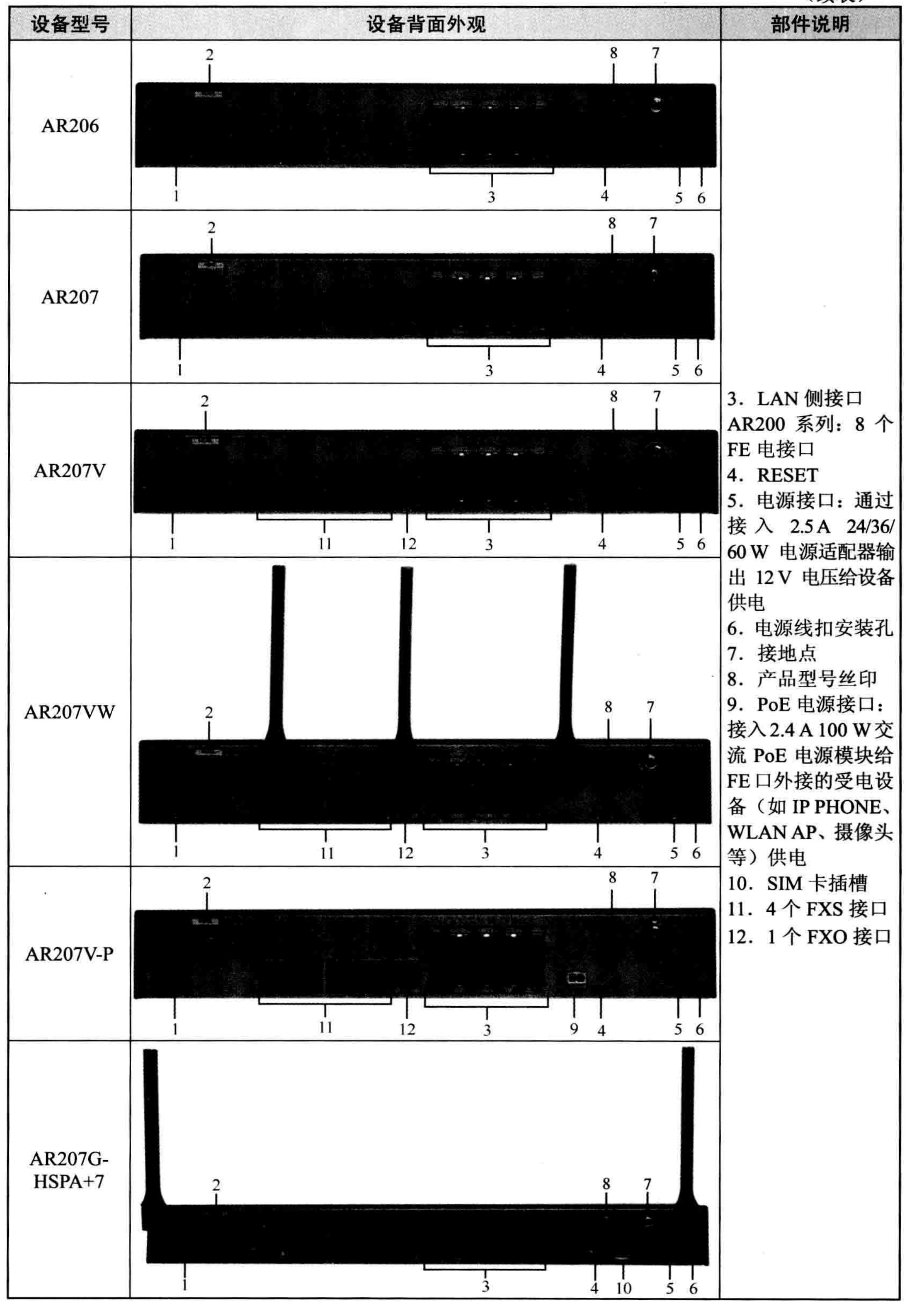
设备型号	设备正面外观	部件说明
AR201、AR206 AR207、AR207V AR207V-P、 AR208E		1．USB 接口 2．Wi-Fi 鞭状天线 3．3G 鞭状天线
AR201VW- PAR207VW		
AR207G-HSPA+7		

表 1-19　　AR200 系列设备背面外观结构



设备型号	设备背面外观	部件说明
AR201		1．CON/AUX 接口（说明：暂不支持 **AUX** 功能） 2．WAN 侧接口 ● AR201、AR201 VW-P：FE 电接口 ● AR206：ADSL2+-B/J 接口 ● AR207、AR207V、AR207VW、AR207V-P、AR207G-HSPA+7：ADSL2+-A/M 接口 ● AR208E：G.SHDSL 接口
AR201VW-P		

（续表）



设备型号	设备背面外观	部件说明
AR206		3．LAN 侧接口 AR200 系列：8 个 FE 电接口 4．RESET 5．电源接口：通过接入 2.5 A 24/36/60 W 电源适配器输出 12 V 电压给设备供电 6．电源线扣安装孔 7．接地点 8．产品型号丝印 9．PoE 电源接口：接入 2.4 A 100 W 交流 PoE 电源模块给 FE 口外接的受电设备（如 IP PHONE、WLAN AP、摄像头等）供电 10．SIM 卡插槽 11．4 个 FXS 接口 12．1 个 FXO 接口
AR207		
AR207V		
AR207VW		
AR207V-P		
AR207G-HSPA+7		

（续表）

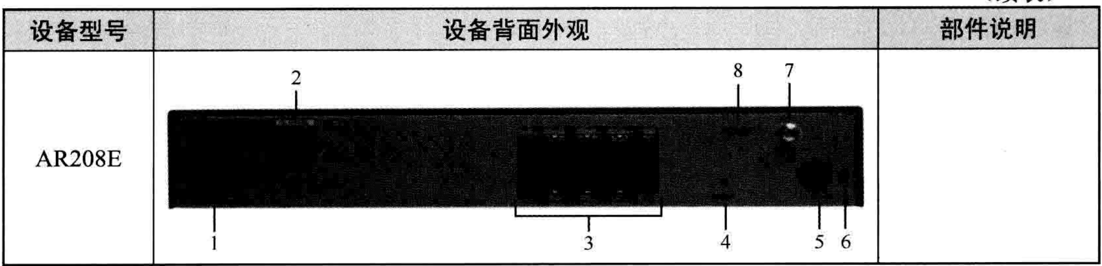
设备型号	设备背面外观	部件说明
AR208E		

表 1-20　**AR200 系列路由器基本配置规格**

规格名称	AR201	AR206	AR207	AR 207V	AR 207V-P	AR208E	AR 201VW-P	AR 207VW	AR207G-HSPA+7
处理器	双核 533 MHz								
转发性能	450 kpps								
带业务转发性能	150 Mbit/s								
支持的 AP 数（本地转发）	—						8		—
支持的并发用户数（本地转发）	—						160		—
固定 WAN 端口	2×FE（其中 1 个 FE 由以太网交换端口提供）	1×ADSL2+ -B/J 1×FE（由以太网交换端口提供）	1×ADSL2+ -A/M 1×FE（由以太网交换端口提供）			1×G.SHDSL 1×FE（由以太网交换端口提供）	2×FE（其中 1 个 FE 由以太网交换端口提供）	1×ADSL2+A/M 1×FE（由以太网交换端口提供）	
固定以太网端口	8×FE								
固定语音接口	—			4×FXS+1×FXO		—	4×FXS+ 1×FXO		—
内置 3G	—								WCDMA HSPA+7
USB2.0 端口	1								
AUX/CON 口	1								
内存容量	512 MB								
Flash	512 MB								
PoE 供电	不支持				支持	不支持	支持	不支持	

1.2.9　AR200 系列路由器指示灯说明

AR200 系列路由器指示灯全部在正面板上，但 AR200 系列不同机型的指示灯不完全相同，具体如表 1-21 所示。

表 1-21　**AR200 系列路由器正面板指示灯**

机型	指示灯
AR201 AR206 AR207 AR208E	AR201、AR206、AR207 和 AR208E 的指示灯除了 WAN 侧接口指示灯丝印不同外，其他都相同。下图是 AR208E 的指示灯，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 1 2 3 4 5 6 7
AR207V AR207V-P	AR207V-P 的指示灯相对于 AR207V，多 1 个 PoE 指示灯，其他都相同。下图是 AR207V-P 的指示灯，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 8 1 2 3 4 5 6 7 13
AR207G-HSPA+7	AR207G-HSPA+7 上的指示灯如下图所示，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 1 2 3 4 5 10 11 12 6 7
AR201VW-P AR207VW	AR201VW-P 的指示灯相对于 AR207VW，多 1 个 PoE 指示灯，其他都相同。下图是 AR20VW-P 的指示灯，各指示灯的含义说明参见表 1-8 中的对应指示灯序号说明 8 1 2 3 4 5 6 9 7 13

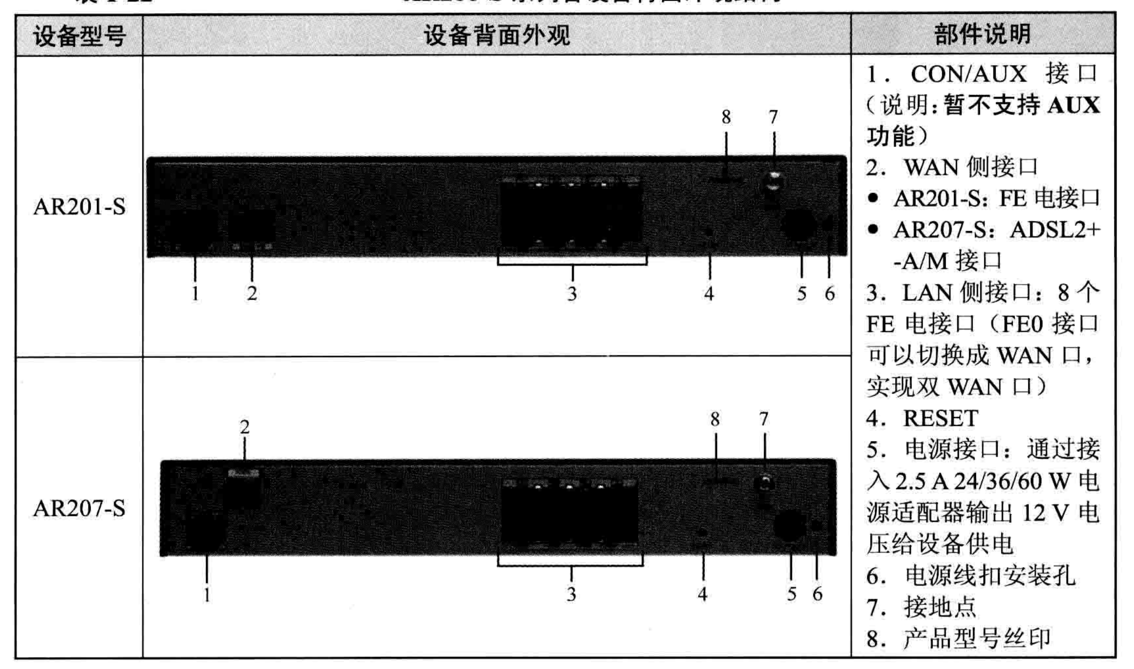
1.2.10　AR200-S 系列产品外观结构及配置规格

AR200-S 系列是 AR200 系列的分销子系列，基本性能与 AR200 系列相当，目前包括两款产品：AR201-S 和 AR207-S。这两款机型的正面外观结构相同，如图 1-9 所示。它们仅对部分 WAN 接入方式提供支持（如 FTTx 光纤接入、ADSL2+），**不支持语音通信**。这些机型名称中各部分的含义请参照本章前面 1.1.3 小节的介绍，背面外观结构如表 1-22 所示，基本配置规格如表 1-23 所示（以官网最新发布为准）。



图 1-9 AR200-S 系列正面外观

表 1-22 **AR200-S 系列各设备背面外观结构**



设备型号	设备背面外观	部件说明
AR201-S	8 7 1 2 3 4 5 6	1．CON/AUX 接口（说明：**暂不支持 AUX 功能**） 2．WAN 侧接口 ● AR201-S：FE 电接口 ● AR207-S：ADSL2+-A/M 接口 3．LAN 侧接口：8 个 FE 电接口（FE0 接口可以切换成 WAN 口，实现双 WAN 口） 4．RESET 5．电源接口：通过接入 2.5 A 24/36/60 W 电源适配器输出 12 V 电压给设备供电 6．电源线扣安装孔 7．接地点 8．产品型号丝印
AR207-S	2 8 7 1 3 4 5 6	

表 1-23 **AR200-S 系列各机型的基本配置规格**

规格名称	AR201-S	AR207-S
处理器	双核 533 MHz	
转发性能	450 kpps	
带业务转发性能	150 Mbit/s	
固定 WAN 端口	2×FE（其中 1 个 FE 由以太网交换端口提供）	1 ADSL2+-A/M，1×FE（由以太网交换端口提供）
固定以太网端口	8×FE	
USB2.0 端口	1	
AUX/CON 口	1	
内存容量	512 MB	
Flash	512 MB	

1.2.11 AR200-S 系列路由器指示灯说明

AR200-S 系列路由器指示灯全部在正面板上，但 AR200-S 系列的两款机型的指示灯状态及含义不完全相同，具体如表 1-24 所示。

表 1-24　**AR200-S 系列路由器正面板指示灯**

机型	指示灯
AR201-S	AR201-S 上的指示灯如下图所示，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 1 2 3 4 5 6 7 HUAWEI
AR207-S	AR207-S 上的指示灯如下图所示，各指示灯及状态含义说明参见表 1-8 中的对应指示灯序号说明 1 2 3 4 5 6 7 HUAWEI

1.2.12　AR150/160/200 系列的基本配置和性能综合比较

尽管 AR150/160/200 系列路由器（包括它们对应的“-S”分销系列）都是面向企业分支和中小型企业的盒式固定接口路由器，但是它们在性能、基本配置和特性支持上还是存在一些区别的。

总体来说，AR150、AR160 和 AR200 系列在性能方面是依次提升的。其中，AR160 系列在许多特性方面没有提供支持，如 WLAN、3G、语音等，所以可以认为它是一个标准型的 AR 系列路由器，但性能方面仍较 AR150 系列有较大提升。这三大系列的基本配置和性能综合比较如表 1-25 所示。从中可以看出，这几个系列都使用了相同的处理器，但转发性能依次提升，**AR160 和 AR150-S、AR200-S 系列均不支持语音通信**。

表 1-25　**AR150/160/200 系列的综合比较**

规格名称	AR150 系列	AR150-S 系列	AR160 系列	AR200 系列	AR200-S 系列
处理器	双核 533 MHz				
转发性能	300 kpps		350 kpps	450 kpps	
带业务转发性能	100 Mbit/s			150 Mbit/s	
固定 WAN 端口	2×FE，或 1ADSL2+-A/M（或 1×ADSL2+-B/J）、1×FE，或 1×G.SHDSL、1×FE		1×G.HSDL（或 1×VDSL2）、1×FE	2×FE 或 1ADSL2+-A/M、1×FE	
固定以太网交换端口	4×FE	4×FE	4×FE	8×FE	8×FE
固定语音接口	AR157VW 提供 4×FXS+1×FXO	-	-	部分机型提供 4×FXS+1×FXO	-
内置 3G	AR151GHSPA+7 和 AR151G-U-S 提供 WCDMA HSPA+7		-	AR207G-SPA+7 提供 WCDMA HSPA+7	-

（续表）

USB2.0 端口	1	1	1	1	1
AUX/CON 端口	1	1	1	1	1
内存容量	512 MB	512 MB	512 MB	512 MB	512 MB
Flash 容量	512 MB	512 MB	512 MB	512 MB	512 MB

1.2.13 AR150/150-S/160/200/200-S 系列路由器的主要应用

AR150/150-S/160/200/200-S 系列路由器的应用非常广泛，远远超出了一般面向中小型企业的路由器所具备的功能与性能。它们的应用主要体现在广域网接入、语音通信、VPN 组网以及 WLAN 接入与管理。不同机型所支持的功能特性参见本章对应小节介绍，下面具体介绍这几个方面的应用。

1. 丰富多样的广域网接入/互连

AR150/160/200 系列企业路由器作为分支用户的出口路由器，支持广域网的各种灵活接入方式，可以进行远程网络互联。有些机型，单一设备就能满足以太网、xDSL、3G、WLAN 等多种接入需求，节约了部署运维成本，灵活地为客户提供了最大价值。这几个系列典型的广域网接入/互联的网络结构如图 1-10 所示。

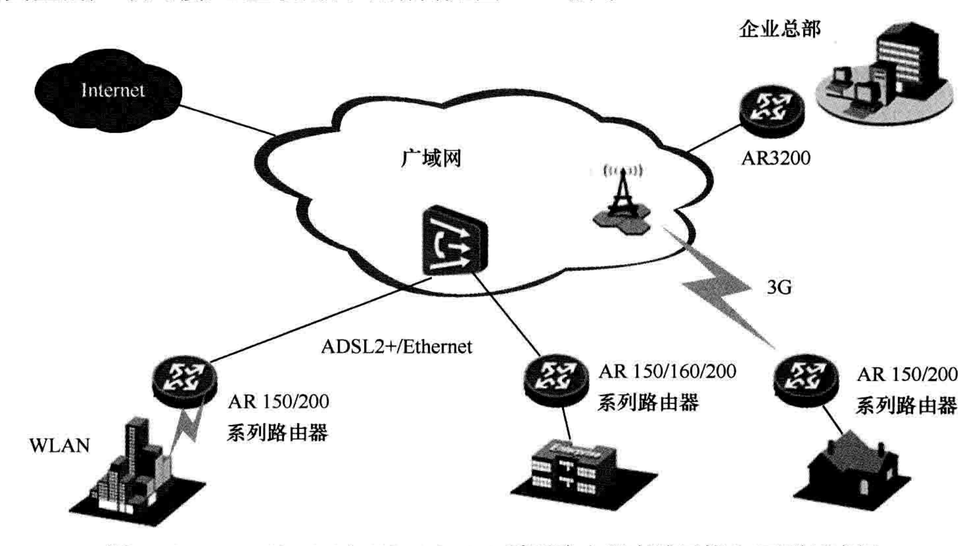


图 1-10 AR150/150-S/160/200/200-S 系列路由器广域网接入/互联示意图

2. 优质融合的语音服务

AR150/150-S/200/200-S 系列企业路由器中的部分机型可用做 IP PBX 和 SIP 接入网关。

在 IP PBX 应用场景，这两个系列的部分机型内置了 PBX，可提供企业总机、IVR 语言导航、话单查询等语音通信业务，可有效提升企业形象，提高企业内外的沟通效率。若这些机型部署在企业分支，同时可支持智能路由拨号功能，则在广域网发生故障时，可使用 PSTN（Public Switched Telephone Network，公共交换电话网络）作为呼叫备份链路；当总部 SIP 服务器不可达时，可通过内置本地 SIP 服务器，实现分支内以及分支与 PSTN 之间的正常通话，保证企业语音业务的可靠性。其典型网络结构如图 1-11 所示。

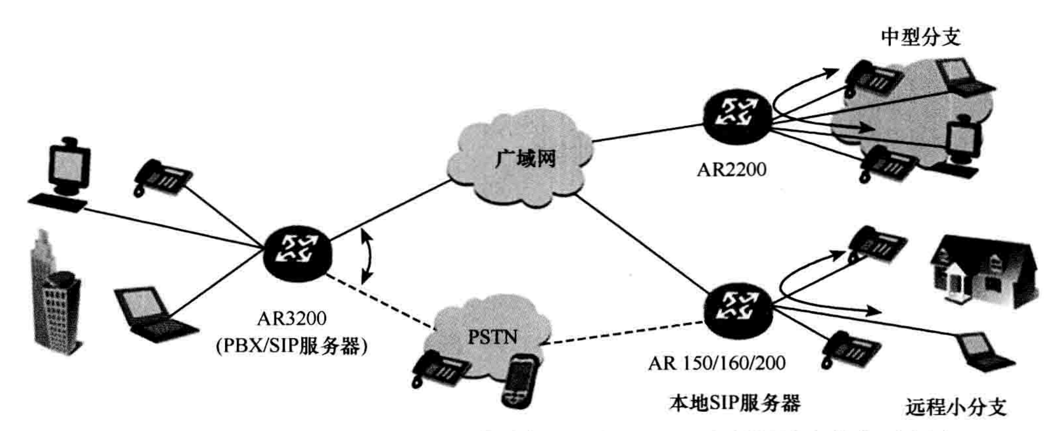


图 1-11　AR150/150-S/200/200-S 系列路由器在 IP PBX 应用场景中的典型应用

在 SIP 接入网关应用场景中，AR150/150-S/200/200-S 系列部分机型可将传统语音、传真与现代 IP 业务有效融合。当运营商为企业部署语音时，AR150/150-S/200/200-S 作为企业分支的 SIP 接入网关，可将普通语音电话信号转化为 VoIP 信号进行呼叫管理。上行与 IMS/NGN 网络互连，实现固话、手机、PC 等任意终端在任意时间的语音通信。其典型网络结构如图 1-12 所示。

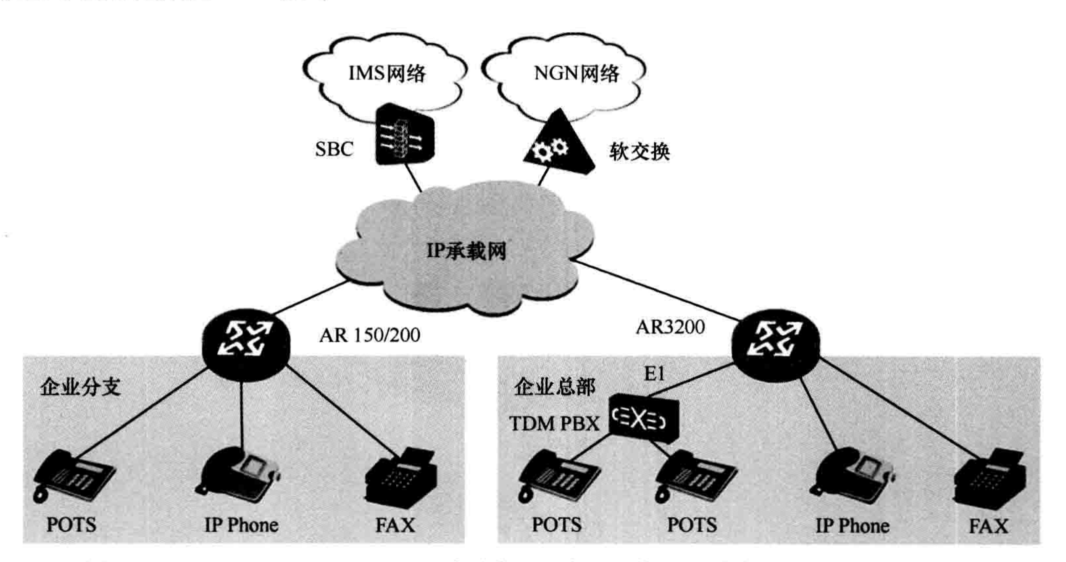


图 1-12　AR150/150-S/200/200-S 系列路由器在 SIP 接入网关应用场景中的典型应用

3. 丰富的企业分支 VPN 组网

AR150/150-S/160/200/200-S 系列企业路由器提供了多种安全接入功能，满足企业分支之间、企业分支与总部之间以及合作伙伴访问企业内部信息的需求。总部和分支机构建立的隧道，包括 GRE VPN、IPSEC VPN、DSVPN、SSL VPN、L2TP VPN 安全隧道，可实现数据的安全访问与传输，支持分支机构侧隧道的快速部署和认证等功能。通过远程隧道接入方式，合作伙伴可灵活访问企业内部资源，实现企业内资源的安全和共享。其典型网络结构如图 1-13 所示。

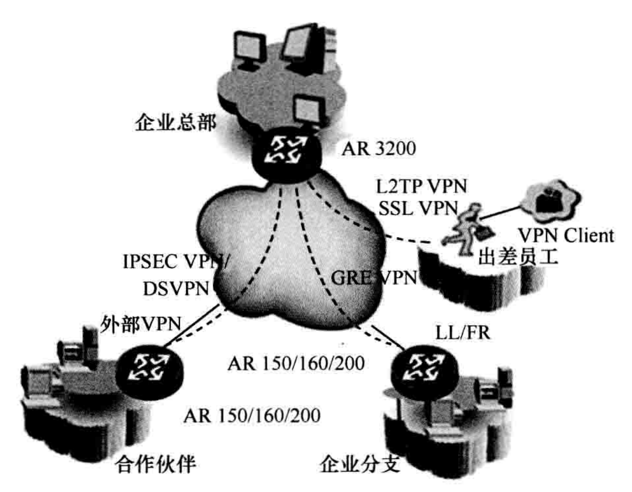


图 1-13 AR150/150-S/160/200/200-S 系列路由器在企业分支 VPN 组网中的典型应用

4. 灵活便捷的无线接入和管理

AR150/200 系列企业路由器的无线接入和管理功能体现在“分支 3G 和 Wi-Fi 无线接入场景”和“无线 AC 管理场景”两方面。

在分支 3G 和 Wi-Fi 无线接入场景中，AR150/150-S/200/200-S 系列企业路由器的部分机型集成了 3G 接入功能，支持 HSPA+的 3G 标准，满足企业分支机构之间以及与总部间的无线互联需求。同时，3G 数据链路可以作为有线链路的备份链路，对 AR 上行的 xDSL、FE/GE、ISDN 等链路提供链路保护，有效提高网络的稳定性，降低网络建设成本。同时，AR150/150-S/200/200-S 系列企业路由器部分机型还集成了 WLAN 无线接入功能，支持 802.11a/b/g/n 标准通信，满足用户的无线接入需求，助力企业灵活构建分支网络。其典型网络结构如图 1-14 所示。

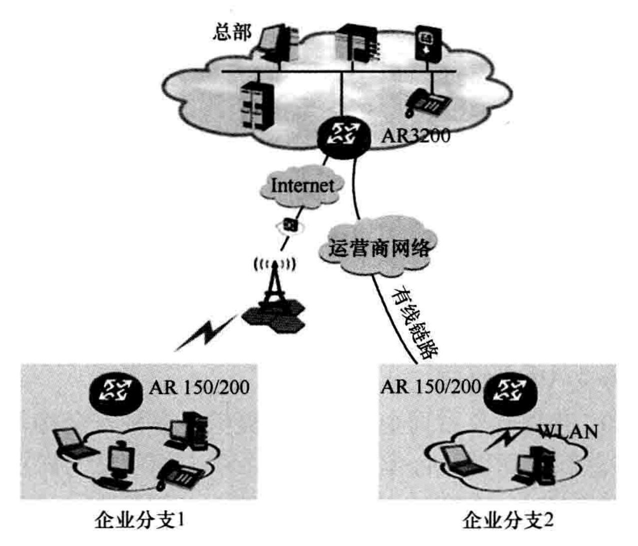


图 1-14 AR150/150-S/200/200-S 系列路由器在分支 3G 和 Wi-Fi 无线接入场景中的典型应用

在无线 AC 管理场景中，AR150/150-S/200/200-S 系列路由器中的部分机型集成了 AC 功能，可对无线局域网中的 AP 进行控制和管理。其支持的丰富认证方式和灵活的用

户权限控制能力，可为 Wi-Fi 用户提供安全接入保证。同时，它们集丰富的无线功能于一身，实现了对有线无线一体化网络的集中管理，满足了不同规模企业的建网要求。其典型网络结构如图 1-15 所示。

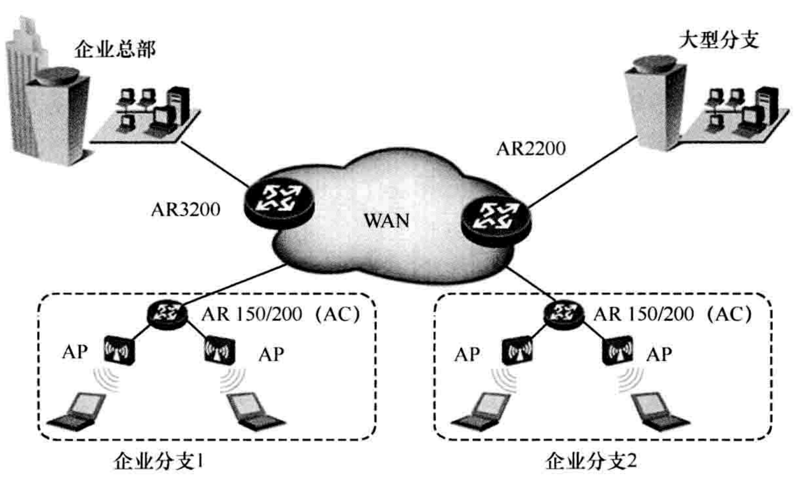


图 1-15　AR150/150-S/200/200-S 系列路由器在无线 AC 管理场景中的典型应用

1.3　AR1200/1200-S/2200/2200-S/3200 系列路由器

AR1200/1200-S/2200/2200-S/3200 系列产品是华为公司推出的新一代多合一模块化结构的企业路由器，提供包括有线和无线的 Internet 接入、专线接入、PBX、融合通信及安全等功能，支持路由、交换、语音、安全、WLAN 等多种融合业务。它们的配置规格和性能是依次增强的，主要应用场景不完全一样。

AR1200/1200-S 系列路由器主要面向中小型办公室或中小型企业分支，可广泛部署于中小型园区网出口、中小型企业总部或分支等场景；AR2200/2200-S 路由器系列主要面向中型企业总部或大中型企业分支，可广泛部署于中型企业总部或分支等场景；AR3200 路由器系列主要面向大中型企业园区网、大中型企业总部或分支，可广泛部署于大中型园区网出口、大中型企业总部或分支等场景。

1.3.1　AR1200/1200-S/2200/2200-S/3200 系列路由器主要特点

AR1200/1200-S/2200/2200-S/3200 系列路由器采用嵌入式硬件加密，支持语音的数字信号处理器（DSP）、防火墙、呼叫处理、语音信箱以及应用程序服务，覆盖业界最广泛的有线和无线连接模式，如 E1/T1、xDSL、xPON、Wi-Fi（仅 AR1200/1200-S 系列部分机型支持）、CPOS（仅 AR2220/AR2220-S/AR2220L/AR2240/AR2240-S/AR3260 系列支持）、3G 接入等。AR1220、1200-S 系列部分机型的百兆固定以太接口还支持 PoE 功能。它们的主要特点如下。

1. 卓越性能，业界领先

AR1200/1200-S/2200/2200-S/3200 系列企业路由器采用多核 CPU 和无阻塞交换架构，

产品性能业界领先，充分满足企业及分支机构网络未来多元化扩展、不断增长的业务需求。具体表现如下。

① 使用多核 CPU，提高数据、语音的并发处理能力，为大容量业务的全方位部署创造条件。

② 无阻塞交换，单槽位总线带宽最大可达 10 Gbit/s，业务转发无瓶颈。

③ 协议管理、业务处理、数据交换独立分布处理，性能更高，业务更可靠。

④ 路由交换一体化，跨板卡交换效率高，配置维护灵活简单。

⑤ 板卡热插拔，风扇等关键硬件冗余设计，保证业务安全稳定。

2. 有线、无线应用一体化，灵活接入

在广域网接入/互联方面，AR1200/1200-S/2200/2200-S/3200 系列支持多种有线和无线接入方式，用户可根据自己的实际应用情况灵活选择。在无线接入方式中，包括以下三种。

① WLAN：内置 AC 功能，低成本构建无线园区，更加灵活。

② 3G：AR1200/1200-S/2200/2200-S 系列全面支持 CDMA2000 EV-DO、WCDMA 的 3G 标准（**AR3200 系列可通过 USB 接口或 SIC 卡提供支持**），保证各种网络的灵活接入；通过 NQA（Network Quality Analyzer，网络质量分析器）技术，可以实时监测链路状态，保证 SLA（Service Level Agreement，服务质量协议）；支持 3G 链路上建立安全 VPN，保证业务安全传输。

③ LTE（Long Term Evolution，长期演进）：LTE 是第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）主导的通用移动通信系统（Universal Mobile Telecommunications System，UMTS）技术的长期演进。LTE 是 3G 的演进，却并非人们普遍认为的 4G 技术，而是 3G 与 4G 技术之间的一个过渡。

目前常见的有线接入方式包括以下几种。

① 光纤接入：包括 GPON 和 EPON 接入方式，支持千兆以太光接口和 CPOS 光接口，灵活匹配网络接入，实现 1 Gbit/s 以上的带宽，充分满足语音等业务高质量大带宽传输的需求。

② 铜缆接入：支持丰富类型的广域网接口类型，如 xDSL、E1/T1、串口、ISDN，上行接入速率从 64 kbit/s 到 1 Gbit/s，使客户可以根据业务需求灵活选择。

3. 多业务合一，融合开放

AR1200/1200-S/2200/2200-S/3200 支持路由、交换、3G、WLAN、语音、安全等功能特性，实现了业务多合一。具体表现在以下几个方面。

① 开放业务平台（OSP）。

通过 OSP 与第三方 IT 系统集成和对接，为企业客户实现统一通信的业务体验，使客户、代理商、第三方和厂家都可以是开发者和使用者，真正实现业务价值链的共赢。

② 丰富语音体验。

集成多种语音功能，利用数据网络满足企业语音通话需求，为企业提供灵活高效的沟通手段。具体包括以下几方面的功能。

- 内置 PBX、SIP 服务器、SIP 接入网关等基础语音功能。
- 提供多方通话、IVR（Interactive Voice Response，交互式语音应答）排队自动接

续、彩铃、同振、顺振、一号通、话单管理、用户管理等丰富的语音增值业务。

- 提供智能呼叫路由等功能，保证语音业务的高可用性。
- QoE（Quality of Experiece，质量体验）功能实时监测诊断语音业务质量。
- 抖动缓冲、回声消除、丢包补偿等机制保证最佳的语音业务体验。

③ 安全业务接入。

AR1200/1200-S/2200/2200-S/3200 系列路由器在业务顺利开展的同时可有效地保障企业网的安全，从用户接入控制、报文检测到主动防御形成一套完整的安全防护机制，实现用户投资回报最大化。具体包括以下安全功能。

- 内置防火墙。
- 支持 802.1x、MAC 地址认证的端口安全机制。
- 实现 Radius、HWTACACS 等多种认证方式。
- 提供 IPSec VPN、GRE VPN、DSVPN、SSL VPN。

4. 智能业务部署

随着企业规模的扩大，客户对业务部署提出了更高的要求。AR1200/1200-S/2200/2200-S/3200 系列路由器采取一系列措施实现业务智能部署。具体包括以下几种。

① 增加 Mini-USB 配置端口，提供 Web 配置方式，界面更加友好。

② U 盘开局，使设备真正可即插即用。

③ Auto-Configure，支持设备自动配置。

5. 简单业务管理

简单管理一直是企业客户关注的重点，AR1200/1200-S/2200/2200-S/3200 系列路由器提供了以下几方面的简化运维措施。

① 与 eSight 网管配套，实现设备管理。

② 通过 NQA 进行链路实时监控，提高运维质量。

③ 支持流检测 NetStream，流量特征可视化，为网规网优提供依据。

1.3.2 AR1200 系列产品外观及配置规格

AR1200 系列目前包含 6 款机型：AR1220、AR1220V、AR1220W、AR1220VW、AR1220L 和 AR1220-D。本系列采用了双核 500 MHz 的更强劲处理器，转发性能达到了 450 kpps，整机交换容量达到 8 Gbit/s，且支持 SIC、WSIC 和 DSP 插槽。这些机型名称中各部分的含义请参照本章前面 1.1.3 小节的介绍，各自的正面外观结构和背面外观结构分别如表 1-26 和表 1-27 所示，各机型的基本配置规格如表 1-28 所示(以官网最新发布为准)。

表 1-26　AR1200 系列设备正面外观结构

设备型号	设备正面外观	部件说明
AR1220 AR1220-D AR1220V AR1220L	1　2	1. USB 接口（说明：插入 3G USB modem 时，同时安装 USB 塑料保护罩（选配）对它进行防护）

（续表）

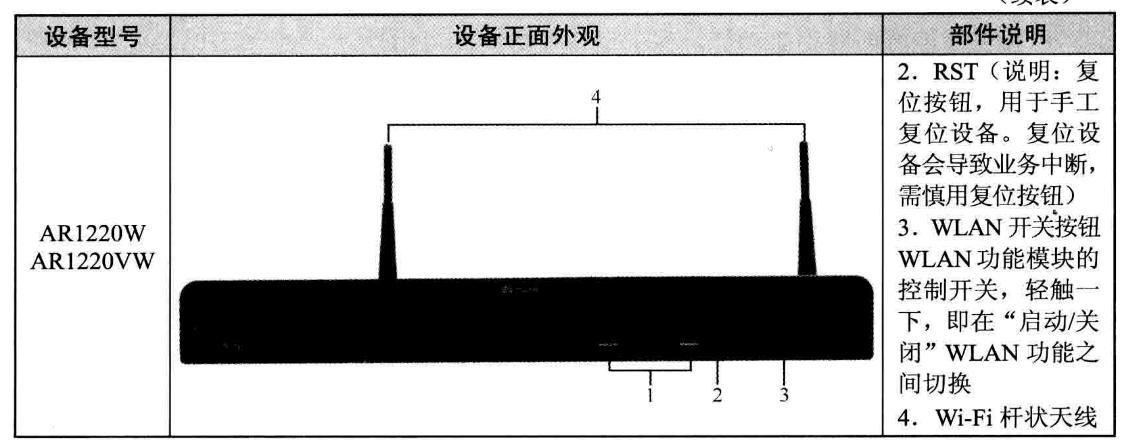
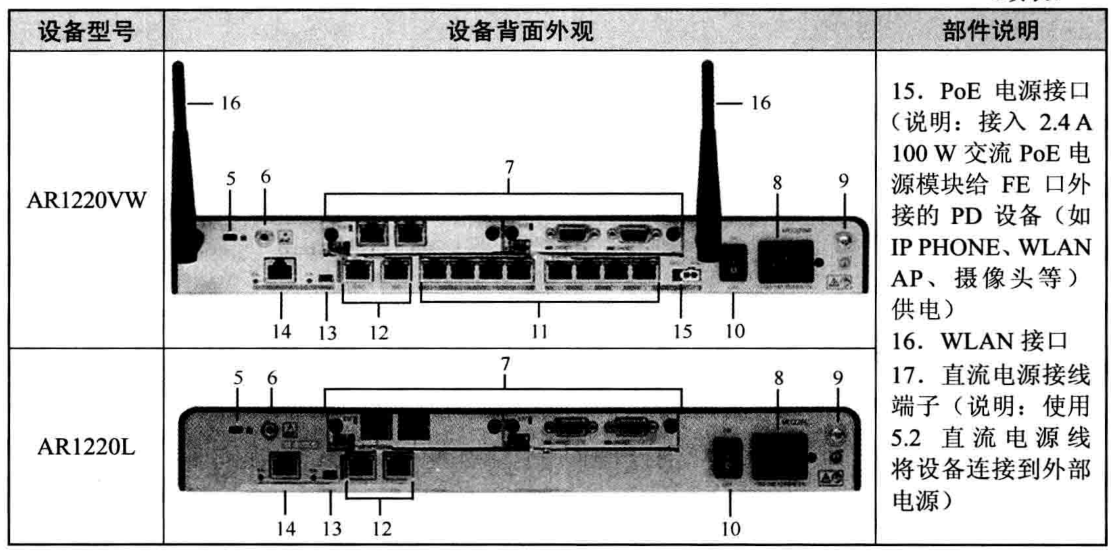
设备型号	设备正面外观	部件说明
AR1220W AR1220VW		2．RST（说明：复位按钮，用于手工复位设备。复位设备会导致业务中断，需慎用复位按钮） 3．WLAN 开关按钮 WLAN 功能模块的控制开关，轻触一下，即在“启动/关闭”WLAN 功能之间切换 4．Wi-Fi 杆状天线

表 1-27　　AR1200 系列设备背面外观结构

设备型号	设备背面外观	部件说明
AR1220		5．防盗锁孔 6．ESD 插孔（说明：对设备进行维护操作时，需要佩戴防静电腕带，防静电腕带的一端要插在 ESD 插孔里） 7．可插拔的单板槽位（说明：AR1200 系列设备支持 2 个 SIC 槽位，2 个 SIC 槽位可以通过拆卸中间的滑道合并成 1 个 WSIC 槽位），**请参见表下面的说明** 8．交流电源线接口（说明：使用 5.1 交流电源线将设备连接到外部电源） 9．接地点（说明：使用 5.3 规格接地线缆将设备可靠接地，防雷、防干扰） 10．电源开关 11．面板上固定的 8 个 FE 电接口 12．面板上固定的 2 个 GE 电接口 13．MiniUSB 接口 14．CON/AUX 接口（说明：AR1200 系列暂不支持 AUX 功能）
AR1220-D		
AR1220V		
AR1220W		

（续表）

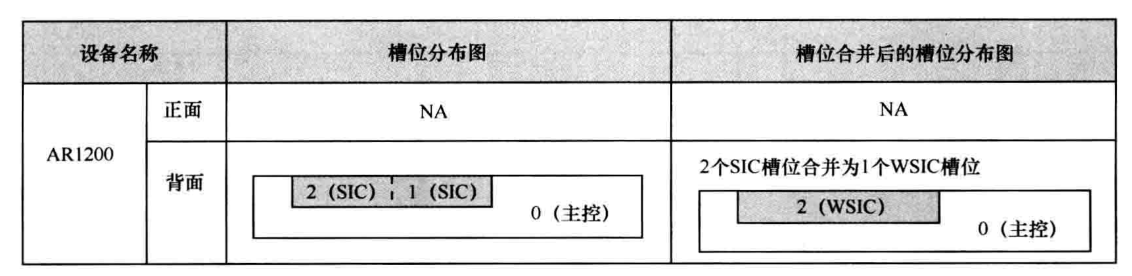


设备型号	设备背面外观	部件说明
AR1220VW	16 16 5 6 7 8 9 14 13 12 11 15 10	15. PoE 电源接口（说明：接入 2.4 A 100 W 交流 PoE 电源模块给 FE 口外接的 PD 设备（如 IP PHONE、WLAN AP、摄像头等）供电） 16. WLAN 接口 17. 直流电源接线端子（说明：使用 5.2 直流电源线将设备连接到外部电源）
AR1220L	5 6 7 8 9 14 13 12 10	

表 1-28　AR1200 系列各机型的基本配置规格

规格名称	AR1220	AR1220V	AR1220W	AR1220VW	AR1220L	AR1220-D
处理器	双核 500 MHz					
转发性能	450 kpps					
带业务转发性能	200 Mbit/s					
整机交换容量	8 Gbit/s					
每槽位交换容量	SIC 和 WSIC 插槽 2 Gbit/s					
固定以太网路由端口	2×GE					
固定以太网交换端口	8×FE				—	8×FE
SIC 插槽	2					
WSIC 插槽（缺省/最大）	0/1（最大槽位数包括由其他槽位合成的槽位数目，下同）					
DSP 插槽	—	缺省支持 32 路语音	—	缺省支持 32 路语音	—	—
Wi-Fi	—	—	支持 802.11b/g/n	支持 802.11b/g/n	—	—
USB2.0 端口	2					
Mini-USB 控制台端口	1					
AUX/CON 端口	1					
内存容量	512 MB					
Flash 容量	256 MB					

说明　AR1200 系列设备槽位分布如图 1-16 所示。两个 SIC 槽位可以通过拆卸滑道合并为 1 个 WSIC 槽位，如槽位 1 和槽位 2 合并为新槽位 2。**但槽位能合不能拆**，槽位合并后的新槽位号取两者中的较大者。



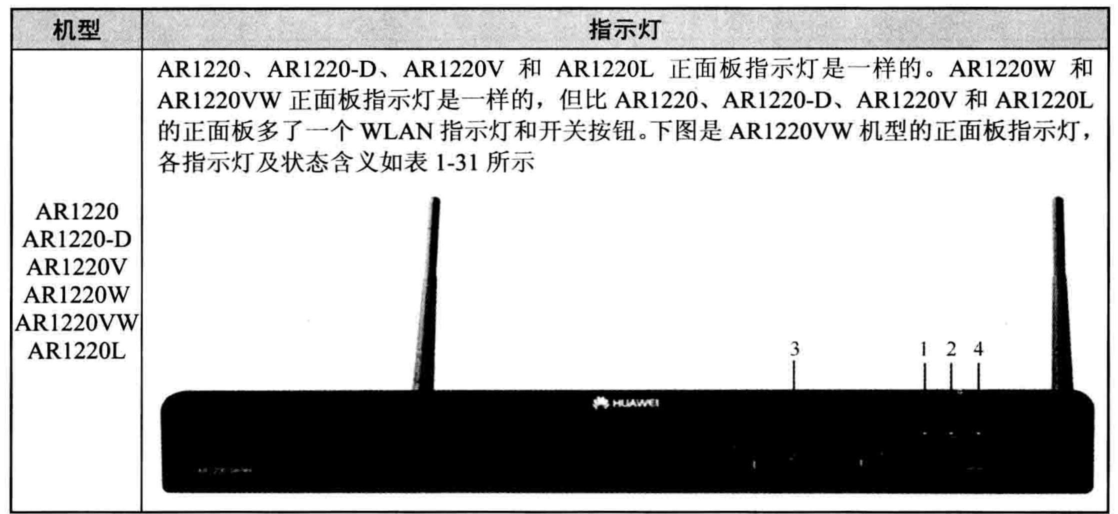
设备名称		槽位分布图	槽位合并后的槽位分布图
AR1200	正面	NA	NA
	背面	2（SIC） 1（SIC） 0（主控）	2个SIC槽位合并为1个WSIC槽位 2（WSIC） 0（主控）

图 1-16 AR1200 系列槽位分布图

1.3.3 AR1200 系列路由器指示灯

AR1200 系列路由器的指示灯与前面介绍的其他几个系列有些区别，在正面板和背面板上都有，且不同设备的指示灯状态及含义有所区别，具体对照关系如表 1-29 和表 1-30 所示。

表 1-29 AR1200 系列设备正面板指示灯



机型	指示灯
AR1220 AR1220-D AR1220V AR1220W AR1220VW AR1220L	AR1220、AR1220-D、AR1220V 和 AR1220L 正面板指示灯是一样的。AR1220W 和 AR1220VW 正面板指示灯是一样的，但比 AR1220、AR1220-D、AR1220V 和 AR1220L 的正面板多了一个 WLAN 指示灯和开关按钮。下图是 AR1220VW 机型的正面板指示灯，各指示灯及状态含义如表 1-31 所示

表 1-30 AR1200 系列设备背面板指示灯

机型	指示灯
AR1220 AR1220-D AR1220V AR1220W AR1220VW AR1220L	AR1220、AR1220-D、AR1220V、AR1220W、AR1220VW 和 AR1220L 背面板指示灯是一样的。下图是 AR1220VW 的背面板指示灯，各指示灯及状态含义如表 1-32 所示 5 6 7 8 9 10

表 1-31 **AR1220VW 面板正面的指示灯及状态说明**

指示灯序号	指示灯/按钮	颜色	指示灯状态及含义
1	SYS	绿色	慢闪：表明系统处于正常运行状态 快闪：表明系统处于上电加载或者复位启动状态
		红色	常亮：表明单板有影响业务且无法自动恢复的故障，需要人工干预
		常灭	红灯、绿灯均不亮，表明软件未运行或处于复位状态
2	WAN	绿色	常亮：表明两个 GE 端口至少有一个端口处于连接/激活状态
			常灭：表明两个 GE 端口都处于未连接/未激活状态
3	ACT（USB）	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，USB 接口故障或者指示灯故障
4	WLAN	绿色	闪烁：表明链路上正在传送数据，闪烁的频率随着流量大小而变化
			常灭：表明链路处于未连接/未激活状态

表 1-32 **AR1220VW 背面板指示灯及状态说明**

指示灯序号	指示灯	颜色	指示灯状态及含义
5	EN（CON/AUX 接口）	绿色	常亮：表明当前是 CON/AUX 接口使能
			常灭：表明当前不是 CON/AUX 接口使能
6	EN（MiniUSB 接口）	绿色	常亮：表明当前是 MiniUSB 接口使能
			常灭：表明当前不是 MiniUSB 接口使能
7 和 8	GE 电接口：绿灯为 LINK，黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
9 和 10	FE 电接口：绿灯为 LINK，黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发

1.3.4 AR1200-S 系列路由器产品外观及配置规格

AR1200-S 是华为公司为分销商定制的 AR1200 系列产品，整体性能与 AR1200 系列相当，也是模块化结构的企业网关路由器。该系列目前包括以下 3 款产品：AR1220-S、AR1220W-S 和 AR1220L-S。它们的正面和背面外观结构分别如表 1-33 和表 1-34 所示，基本配置规格如表 1-35 所示（以官网最新发布为准）。

表 1-33 **AR1200-S 系列设备正面外观结构**

机型	设备正面外观	部件说明
AR1220-S AR1220L-S	1 2	1．USB 接口（说明：插入 3G USB modem 时，同时安装 USB 塑料保护罩（选配）对它进行防护）

（续表）

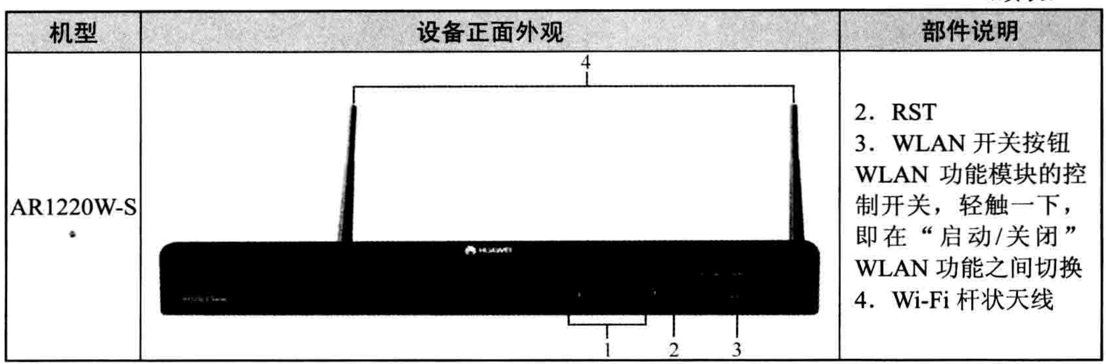
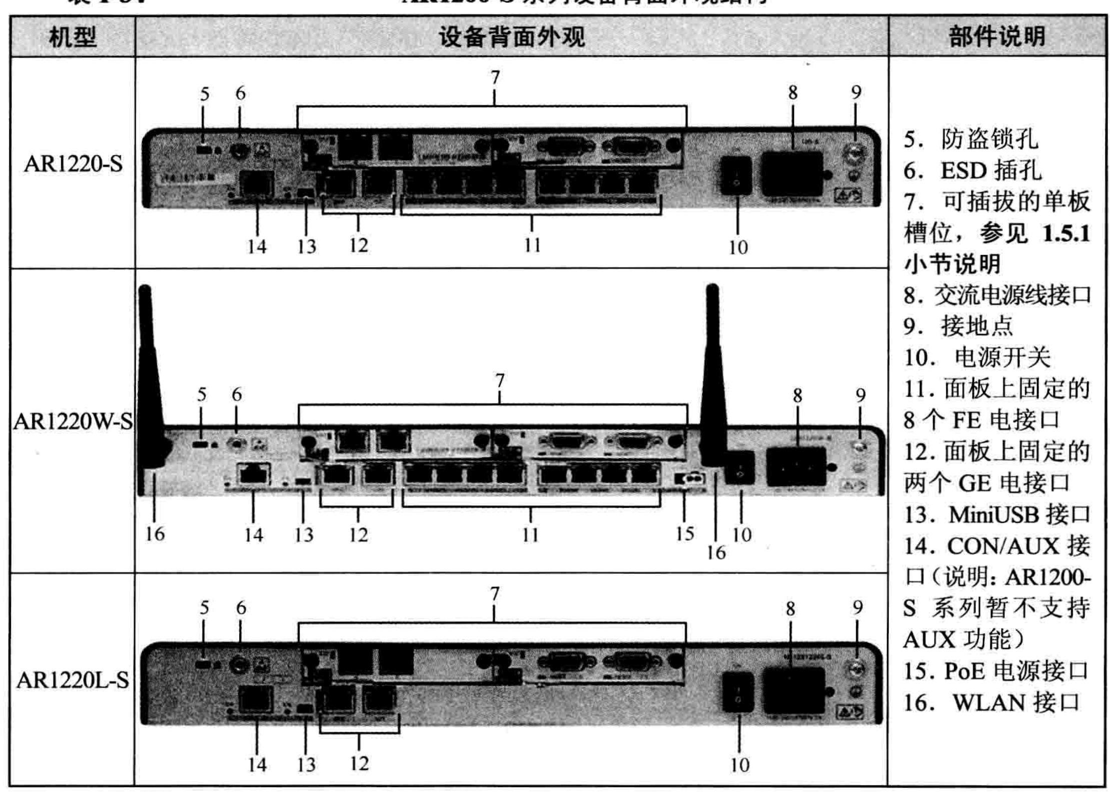
机型	设备正面外观	部件说明
AR1220W-S		2．RST 3．WLAN 开关按钮 WLAN 功能模块的控制开关，轻触一下，即在“启动/关闭”WLAN 功能之间切换 4．Wi-Fi 杆状天线

表 1-34　AR1200-S 系列设备背面外观结构



机型	设备背面外观	部件说明
AR1220-S		5．防盗锁孔 6．ESD 插孔 7．可插拔的单板槽位，**参见 1.5.1 小节说明** 8．交流电源线接口 9．接地点 10．电源开关 11．面板上固定的 8 个 FE 电接口 12．面板上固定的两个 GE 电接口 13．MiniUSB 接口 14．CON/AUX 接口（说明：AR1200-S 系列暂不支持 AUX 功能） 15．PoE 电源接口 16．WLAN 接口
AR1220W-S		
AR1220L-S		

表 1-35　AR1200-S 系列各机型的基本配置规格

规格名称	AR1220L-S	AR1220-S	AR1220W-S
处理器	双核 500 MHz		
转发性能	450 kpps		
带业务转发性能	200 Mbit/s		
整机交换容量	8 Gbit/s		
固定以太网路由端口	2×GE		
固定以太网交换端口	—	8×FE	
SIC 插槽	2		

（续表）

WSIC 插槽（缺省/最大）	0/1	
WIFI	—	支持 802.11 b/g/n
USB2.0 端口	2	
Mini-USB 控制台端口	1	
AUX/CON 端口	1	
内存容量	512 MB	
Flash 容量	256 MB	

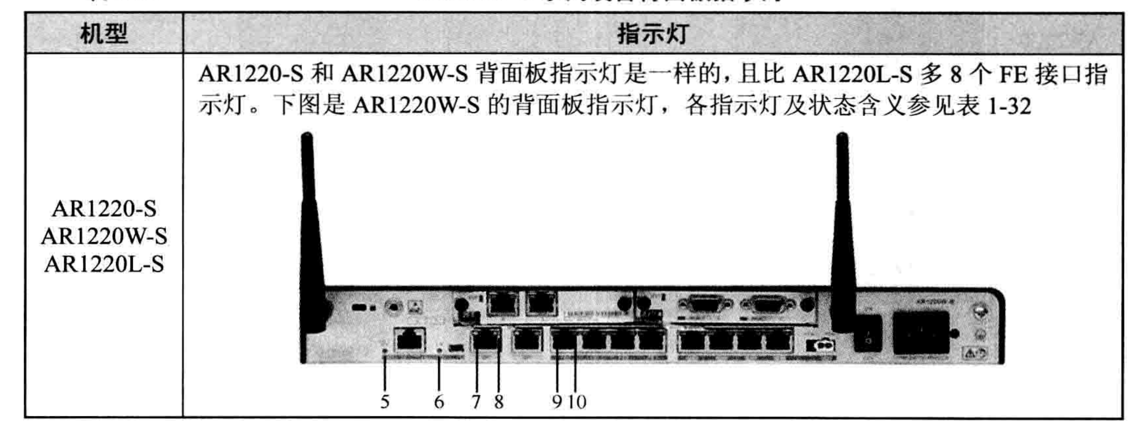
1.3.5　AR1200-S 系列路由器指示灯

AR1200-S 系列路由器的指示灯与前面介绍的 AR1200 系列一样，也在正面板和背面板上都有，但不同机型的指示灯状态及含义有所区别，具体对照关系如表 1-36 和表 1-37 所示。

表 1-36　**AR1200-S 系列设备正面板指示灯**

机型	指示灯
AR1220-S AR1220W-S AR1220L-S	AR1220-S 和 AR1220L-S 正面板指示灯是一样的。AR1220W-S 正面板指示灯只比 AR1220-S 和 AR1220L-S 多了一个 WLAN 指示灯和开关按钮。下图是 AR1220W-S 机型的正面板指示灯，各指示灯及状态含义参见表 1-31 3　1 2 4

表 1-37　**AR1200-S 系列设备背面板指示灯**

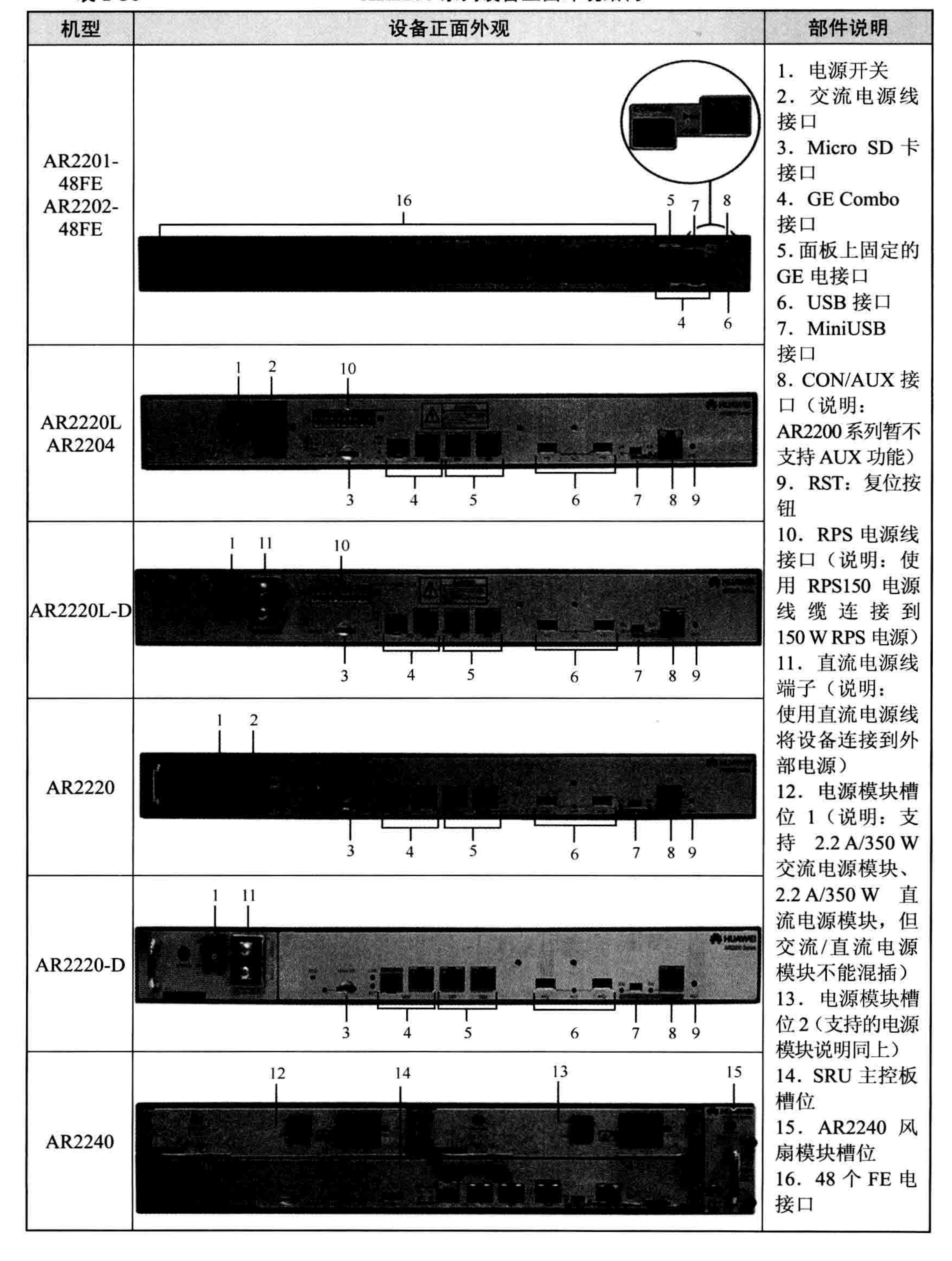
机型	指示灯
AR1220-S AR1220W-S AR1220L-S	AR1220-S 和 AR1220W-S 背面板指示灯是一样的，且比 AR1220L-S 多 8 个 FE 接口指示灯。下图是 AR1220W-S 的背面板指示灯，各指示灯及状态含义参见表 1-32 

1.3.6　AR2200 系列路由器产品外观及配置规格

AR2200 系列目前包含 8 款机型：AR2201-48FE、AR2202-48FE、AR2204、AR2220、

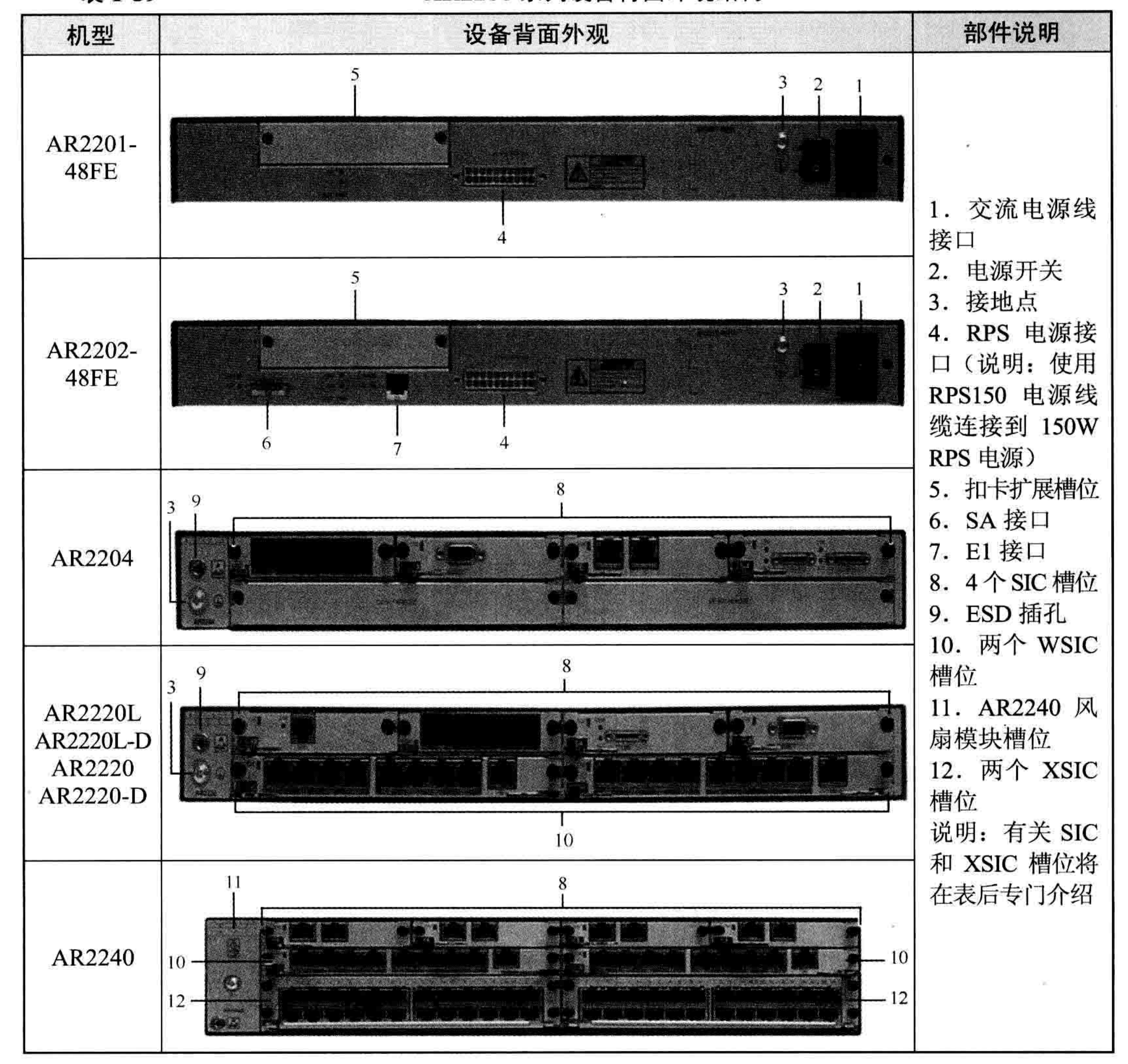
AR2220-D、AR2220L、AR2220L-D 和 AR2240。它们各自的正面外观和背面外观结构分别如表 1-38 和表 1-39 所示。它们各自的基本配置规格如表 1-40 所示（以官网发布的为准）。

表 1-38　　AR2200 系列设备正面外观结构



机型	设备正面外观	部件说明
AR2201-48FE AR2202-48FE	16, 5, 7, 8, 4, 6	1．电源开关 2．交流电源线接口 3．Micro SD 卡接口 4．GE Combo 接口 5．面板上固定的 GE 电接口 6．USB 接口 7．MiniUSB 接口 8．CON/AUX 接口（说明：AR2200 系列暂不支持 AUX 功能） 9．RST：复位按钮 10．RPS 电源线接口（说明：使用 RPS150 电源线缆连接到 150 W RPS 电源） 11．直流电源线端子（说明：使用直流电源线将设备连接到外部电源） 12．电源模块槽位 1（说明：支持 2.2 A/350 W 交流电源模块、2.2 A/350 W 直流电源模块，但交流/直流电源模块不能混插） 13．电源模块槽位 2（支持的电源模块说明同上） 14．SRU 主控板槽位 15．AR2240 风扇模块槽位 16．48 个 FE 电接口
AR2220L AR2204	1, 2, 10, 3, 4, 5, 6, 7, 8, 9	
AR2220L-D	1, 11, 10, 3, 4, 5, 6, 7, 8, 9	
AR2220	1, 2, 3, 4, 5, 6, 7, 8, 9	
AR2220-D	1, 11, 3, 4, 5, 6, 7, 8, 9	
AR2240	12, 14, 13, 15	

表 1-39　　**AR2200** 系列设备背面外观结构



机型	设备背面外观	部件说明
AR2201-48FE		1．交流电源线接口 2．电源开关 3．接地点 4．RPS 电源接口（说明：使用 RPS150 电源线缆连接到 150W RPS 电源） 5．扣卡扩展槽位 6．SA 接口 7．E1 接口 8．4 个 SIC 槽位 9．ESD 插孔 10．两个 WSIC 槽位 11．AR2240 风扇模块槽位 12．两个 XSIC 槽位 说明：有关 SIC 和 XSIC 槽位将在表后专门介绍
AR2202-48FE		
AR2204		
AR2220L AR2220L-D AR2220 AR2220-D		
AR2240		

表 1-40　　**AR2200** 系列路由器基本配置规格

规格名称	AR2201-48FE/2202-48FE	AR2204	AR2220L/2220L-D	AR2220/2220-D	AR2240
处理器	双核 533 MHz	双核 800 MHz		四核 600 MHz	SRU40：8 核 600 MHz SRU60：8 核 600 MHz SRU80：12 核 750 MHz
转发性能	350 kpps	450 kpps	600 kpps	2.5 Mpps	5 Mpps～20 Mpps
带业务转发性能	200 Mbit/s			400 Mbit/s	600 Mbit/s～4.5 Gbit/s
整机交换容量	—	10 Gbit/s	14 Gbit/s	32 Gbit/s	80 Gbit/s
固定以太网路由端口	2×GE (1×Combo)，2×FE（由以太网交换端口提供）	3×GE (1×Combo)			3×GE (2×Combo)/4×GE Combo+ 2×10GE
SIC 插槽	0	4			

（续表）

<table>
<tr><td>WSIC 插槽（缺省/最大）</td><td>0</td><td>0/2</td><td colspan="3">2/4</td></tr>
<tr><td>XSIC 插槽（缺省/最大）</td><td colspan="2">0</td><td colspan="2">0/2</td><td>2/4</td></tr>
<tr><td>EXSIC 插槽（与 XSIC 共享插槽）</td><td colspan="4">0</td><td>1</td></tr>
<tr><td>DSP 插槽</td><td>0</td><td colspan="2">2</td><td>1</td><td>0/3</td></tr>
<tr><td>USB2.0 端口</td><td>1</td><td colspan="3">2</td><td>1/2</td></tr>
<tr><td>Mini-USB 控制台端口</td><td colspan="5">1</td></tr>
<tr><td>AUX/CON 端口</td><td colspan="5">1</td></tr>
<tr><td>内存容量</td><td>512 MB</td><td colspan="2">1 GB</td><td colspan="2">2 GB/4 GB</td></tr>
<tr><td>Flash（缺省/最大）</td><td>512 MB</td><td colspan="2">512 MB /4 GB</td><td colspan="2">2 GB/4 GB</td></tr>
</table>

说明 AR2200 系列设备槽位分布如图 1-17 和图 1-18 所示。但 AR2201-48FE 和 AR2202-48FE 设备不支持 SIC 卡槽位。

① 两个 SIC 槽位可以通过拆卸滑道合并为一个 WSIC 槽位。

② 两个 SIC 槽位+下面的 WSIC 槽位可以通过拆卸滑道合并为一个 XSIC 槽位。

③ 两个 XSIC 槽位可以通过拆卸滑道合并为一个 EXSIC 槽位。

但槽位能合不能拆，槽位合并后的新槽位号取两者中的较大者。

V200R002C00 版本采用了特制的结构件，XSIC 槽位可以插一块 WSIC 卡，插在 XSIC 槽位的下半边，WSIC 卡的槽位号还是原 XSIC 槽位号。

<table>
<tr><th colspan="2">设备名称</th><th>槽位分布图</th><th>槽位合并后的槽位分布图</th></tr>
<tr><td rowspan="2">AR2204</td><td>正面</td><td>NA</td><td>NA</td></tr>
<tr><td>背面</td><td>4（SIC） 3（SIC） 2（SIC） 1（SIC）
NA NA</td><td>2个SIC槽位合并为1个WSIC槽位
4（WSIC） 2（WSIC）
NA NA</td></tr>
</table>

图 1-17 AR2204 槽位分布图

各 AR2200 系列设备的槽位可以进行以下合并操作。

① 在 AR2204 上可以将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽位 4。

② 在 AR2220L 和 AR2220 上可以将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽位 4；将新槽位 2 和槽位 5 合并为新槽位 5；将新槽位 4 和槽位 6 合并为新槽位 6。

③ 在 AR2240 上可以将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽位 4；将新槽位 2 和槽位 5 合并为新槽位 5；将新槽位 4 和槽位 6 合并为新槽位 6；

将槽位 7 和槽位 8 合并为新槽位 8。

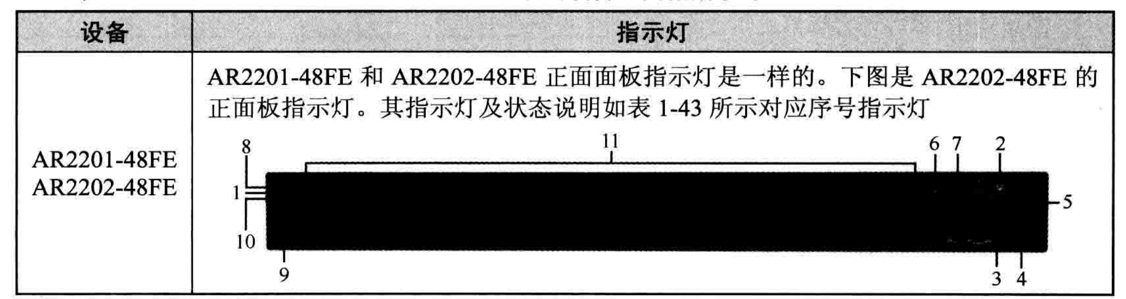
设备名称		槽位分布图	槽位合并后的槽位分布图
AR2220L /AR2220	正面	NA	NA
	背面	4（SIC） 3（SIC） 2（SIC） 1（SIC） 6（WSIC） 5（WSIC）	2个SIC槽位合并为1个WSIC槽位 4（WSIC） 2（WSIC） 6（WSIC） 5（WSIC） 2个WSIC槽位合并为1个XSIC槽位 6（XSIC） 5（XSIC）
AR2240	正面	10（电源） 9（电源） 11（主控） 风扇框	NA
	背面	4（SIC） 3（SIC） 2（SIC） 1（SIC） 6（WSIC） 5（WSIC） 8（XSIC） 7（XSIC）	2个SIC槽位合并为1个WSIC槽位 4（WSIC） 2（WSIC） 6（WSIC） 5（WSIC） 8（XSIC） 7（XSIC） 2个WSIC槽位合并为1个XSIC槽位 6（XSIC） 5（XSIC） 8（XSIC） 7（XSIC） 2个XSIC槽位合并为1个EXSIC槽位 6（XSIC） 5（XSIC） 8（EXSIC）

图 1-18　AR2220L、AR2220 和 AR2240 槽位分布图

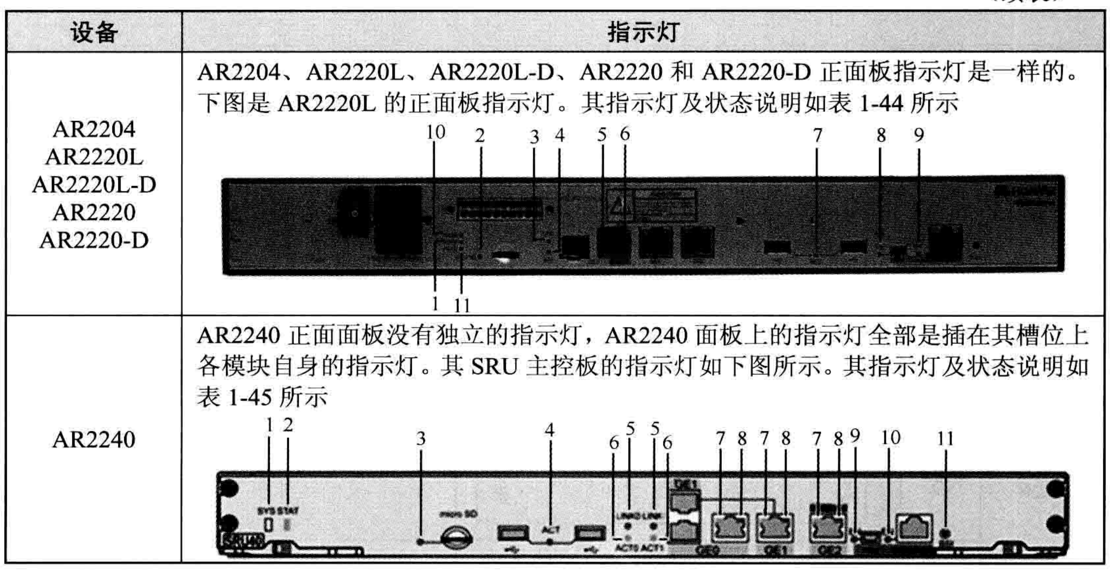
1.3.7　AR2200 系列路由器指示灯

AR2200 系列路由器在正面板和背面板上也都均有指示灯，且不同机型设备的指示灯状态及含义有所区别，具体对照关系如表 1-41 和表 1-42 所示。

表 1-41　AR2200 系列设备正面板指示灯

设备	指示灯
AR2201-48FE AR2202-48FE	AR2201-48FE 和 AR2202-48FE 正面面板指示灯是一样的。下图是 AR2202-48FE 的正面板指示灯。其指示灯及状态说明如表 1-43 所示对应序号指示灯 

（续表）



设备	指示灯
AR2204 AR2220L AR2220L-D AR2220 AR2220-D	AR2204、AR2220L、AR2220L-D、AR2220 和 AR2220-D 正面板指示灯是一样的。下图是 AR2220L 的正面板指示灯。其指示灯及状态说明如表 1-44 所示
AR2240	AR2240 正面面板没有独立的指示灯，AR2240 面板上的指示灯全部是插在其槽位上各模块自身的指示灯。其 SRU 主控板的指示灯如下图所示。其指示灯及状态说明如表 1-45 所示

表 1-42　　AR2200 系列设备背面板指示灯

机型	指示灯
AR2201-48FE AR2202-48FE	AR2202-48FE 比 AR2201-48FE 面板背面多一个 SA 和 E1 指示灯，其他指示灯一样。下图是 AR2202-48FE 的背面板指示灯。其指示灯及状态说明参见表 1-43 中的对应序号指示灯说明
AR2204 AR2220L AR2220L-D AR2220 AR2220-D AR2240	AR2204、AR2220L、AR2220L-D、AR2220、AR2220-DAR2240 背面面板上没有独立的指示灯，面板上的指示灯全部是插在其槽位上各单板自身的指示灯，请参见产品手册中各业务单板指示灯说明

表 1-43　　AR2202-48FE 面板指示灯及状态说明

指示灯序号	指示灯	颜色	指示灯状态及含义
1	SYS	绿色	• 慢闪：表明系统处于正常运行状态 • 快闪：表明系统处于上电加载或者复位启动状态
		红色	常亮：表明单板有影响业务且无法自动恢复的故障，需要人工干预
		常灭	红灯、绿灯均不亮：表明软件未运行或处于复位状态
2	EN（CON/AUX 端口）	绿色	常亮：表明当前是 CON/AUX 端口使能
			常灭：表明当前不是 CON/AUX 端口使能
3	EN（SFP 光口）	绿色	• 常亮：表明 SFP 光口已经连通 • 闪烁：SFP 光口有数据收发 • 常灭：表明 SFP 光口无链接

（续表）

指示灯序号	指示灯	颜色	指示灯状态及含义
4	ACT（USB）	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，USB 接口故障或者指示灯故障
5	EN（MiniUSB 端口）	绿色	• 常亮：表明当前是 MiniUSB 端口使能 • 常灭：表明当前不是 MiniUSB 端口使能
6 和 7	GE 端口：绿灯为 LINK，黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
8	PWR	绿色	AR 内部电源供电正常
		常灭	设备未上电
9	RPS	绿色	常亮：RPS 电源在位
		黄色	常亮：RPS 电源已连接但状态异常
			闪烁：RPS 电源正在给设备供电
		常灭	RPS 电源未连接
10	WAN	绿色	常亮：WAN 处于连接/激活状态
			常灭：WAN 处于未连接/未激活状态
11	48FE 端口	绿色	常亮：表明 FE 端口已经连通
			闪烁：表明 FE 端口有数据传送
			常灭：表明 FE 端口无链接
12 和 13	SA 端口： • 上面为 LINK，绿色 • 下面为 ACT，黄色	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
14 和 15	E1 端口： • 上面为 LINK，绿色 • 下面为 ACT，黄色	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发

表 1-44　　AR2220L 正面板指示灯及状态说明

指示灯序号	指示灯	颜色	指示灯状态及含义
1	SYS	绿色	慢闪：表明系统处于正常运行状态 快闪：表明系统处于上电加载或者复位启动状态
		红色	常亮：表明单板有影响业务且无法自动恢复的故障，需要人工干预
		常灭	红灯、绿灯均不亮，表明软件未运行或处于复位状态
2	Micro SD 卡指示灯	绿色	常亮：表明链路已经连通
			闪烁：表明有数据收发
			常灭：表明无卡

（续表）

指示灯序号	指示灯	颜色	指示灯状态及含义
3 和 4	SFP 端口： • 上面为 LINK，绿色 • 下面为 ACT，黄色	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
5 和 6	GE 端口：绿灯为 LINK，黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
7	ACT（USB）	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，USB 接口故障或者指示灯故障
8	EN（MiniUSB 端口）	绿色	常亮：表明当前是 MiniUSB 端口使能
			常灭：表明当前不是 MiniUSB 端口使能
9	EN（CON/AUX 端口） 说明：CON/AUX 端口和 MiniUSB 端口是复用的，同一时刻只有一个可以使用。缺省情况下，CON/AUX 端口有效，对应的 EN 指示灯绿色常亮，不管是否插线缆	绿色	常亮：表明当前是 CON/AUX 端口使能
			常灭：表明当前不是 CON/AUX 端口使能
10	PWR	绿色	AR 内部电源供电正常
		红色	AR 内部电源供电异常
		常灭	设备未上电
11	RPS	绿色	常亮：RPS 电源在位
		黄色	常亮：RPS 电源已连接但状态异常
			闪烁：RPS 电源正在给设备供电
		常灭	RPS 电源未连接

表 1-45　　SRU 主控上的指示灯及状态说明

指示灯序号	指示灯	颜色	含义
1	SYS	绿色	• 慢闪（0.5 Hz）：表明系统处于正常运行状态 • 快闪（4 Hz）：表明系统处于上电加载或者复位启动状态
		红色	常亮：表明单板有影响业务且无法自动恢复的故障，需要人工干预
		常灭	红灯、绿灯均不亮，表明软件未运行或处于复位状态
2	ACT（主备用指示灯） 说明：AR2240 只能插一块 SRU 主控板，直接作为主用	绿色	常亮：表明该 SRU 主控板处于主用状态
			常灭：表明该 SRU 主控板处于备用状态

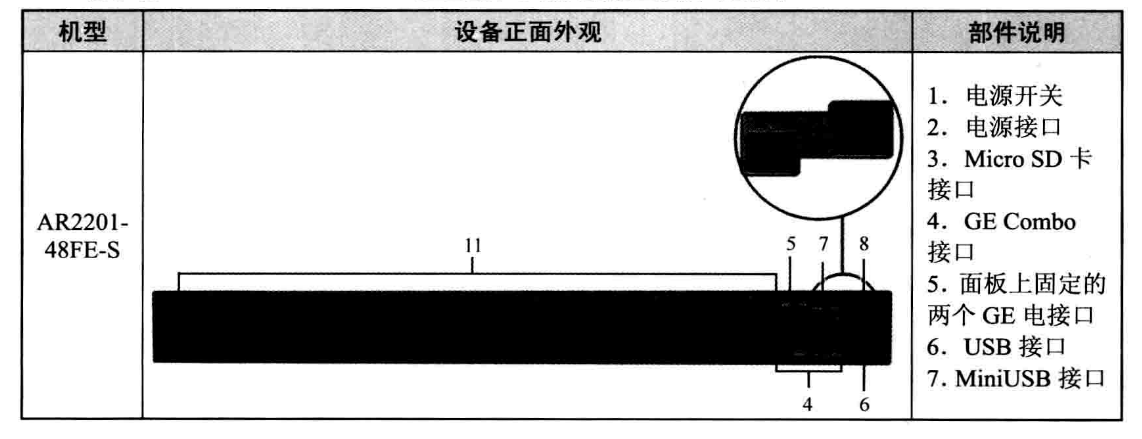
（续表）

指示灯序号	指示灯	颜色	含义
3	Micro SD	绿色	常亮：表明链路已经连通
			闪烁：表明有数据收发
			常灭：表明无 SD 卡
4	ACT（USB）	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，USB 接口故障或者指示灯故障
5 和 6	SFP 端口： • 上面为 LINK，绿色 • 下面为 ACT，黄色	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
7 和 8	GE 端口： • 绿灯为 LINK • 黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
9	MiniUSB EN	绿色	常亮：表明当前是 MiniUSB 端口使能
			常灭：表明当前不是 MiniUSB 端口使能
10	CON/AUX EN	绿色	常亮：表明当前是 CON/AUX 端口使能
			常灭：表明当前不是 CON/AUX 端口使能
11	RST	复位按钮，用于手工复位单板。复位单板会导致业务中断，需慎用复位按钮	

1.3.8　AR2200-S 系列路由器产品外观及配置规格

AR2200-S 是华为公司为分销商定制的 AR2200 系列产品，其整体性能与 AR2200 系列相当，也是模块化结构的企业网关路由器。该系列目前包括 4 款产品：AR2201-48FE-S、AR2204-S\AR2220-S 和 AR2240-S。它们的正面和背面外观结构分别如表 1-46 和表 1-47 所示，基本的配置规格如表 1-48 所示（以官网最新发布为准）。

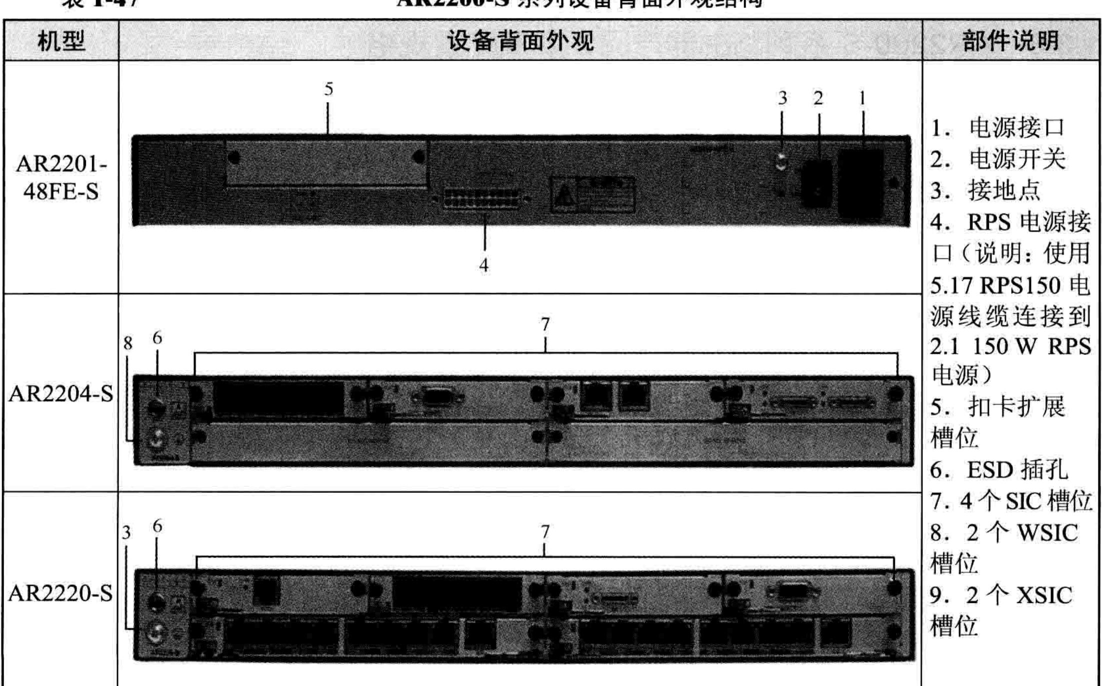
表 1-46　AR2200-S 系列设备正面外观结构

机型	设备正面外观	部件说明
AR2201-48FE-S		1．电源开关 2．电源接口 3．Micro SD 卡接口 4．GE Combo 接口 5．面板上固定的两个 GE 电接口 6．USB 接口 7. MiniUSB 接口

（续表）

机型	设备正面外观	部件说明
AR2204-S	1 2 10 3 4 5 6 7 8 9	8．CON/AUX 接口（说明：AR2200-S 系列不支持 AUX 功能） 9．RST 10．RPS 电源接口（说明：使用 5.17 RPS150 电源线缆连接到 2.1 150 W RPS 电源 11．48 个 FE 电接口 12．电源模块槽位 1（支持 2.2 A/350 W 交流电源模块） 13．电源模块槽位 2（电源模块支持说明同上） 14．AR2240-S 风扇模块槽位 15．SRU 主控板槽位
AR2220-S	1 2 3 4 5 6 7 8 9	
AR2240-S	12 13 14 15	

表 1-47　AR2200-S 系列设备背面外观结构

机型	设备背面外观	部件说明
AR2201-48FE-S	 5 3 2 1 4	1．电源接口 2．电源开关 3．接地点 4．RPS 电源接口（说明：使用 5.17 RPS150 电源线缆连接到 2.1 150 W RPS 电源） 5．扣卡扩展槽位 6．ESD 插孔 7．4 个 SIC 槽位 8．2 个 WSIC 槽位 9．2 个 XSIC 槽位
AR2204-S	8 6 7	
AR2220-S	3 6 7	

（续表）

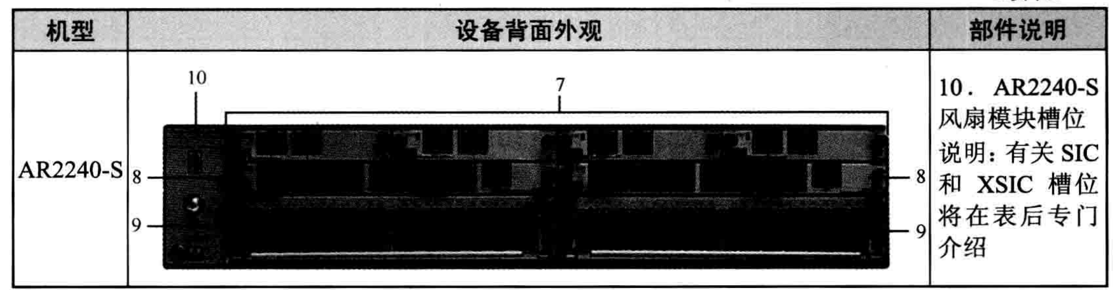
机型	设备背面外观	部件说明
AR2240-S		10．AR2240-S 风扇模块槽位 说明：有关 SIC 和 XSIC 槽位将在表后专门介绍

表 1-48 **AR2200-S** 系列路由器基本配置规格

规格名称	AR2201-48FE-S	AR2204-S	AR2220-S	AR2240-S
处理器	双核 533 MHz	双核 800 MHz	四核 600 MHz	SRU40：8 核 600 MHz
转发性能	350 kpps	450 kpps	1 Mpps	2 Mpps
带业务转发性能	200 Mbit/s		400 Mbit/s	600 Mbit/s
整机交换容量	—	10 Gbit/s	32 Gbit/s	80 Gbit/s
固定以太网路由端口	2×GE (1×Combo)，2×FE（由以太网交换端口提供）	3×GE (1×Combo)		3×GE (2×Combo)
SIC 插槽	0	4		
WSIC 插槽（缺省/最大）	0	0/2	2/4	
XSIC 插槽（缺省/最大）	0		0/2	2/4
EXSIC 插槽（与 XSIC 共享插槽）	0			1
DSP 插槽	0	2	1	3
USB2.0 端口	1	2		
Mini-USB 控制台端口	1			
AUX/CON 端口	1			
内存容量	512 MB	1 GB	2 GB	
Flash（缺省/最大）	512 MB		16 MB	
Micro SD	—	-/4 GB	2 GB/4 GB	

说明 AR2200-S 系列各机型设备槽位分布如图 1-19 和图 1-20 所示。两个 SIC 槽位可以通过拆卸滑道合并为一个 WSIC 槽位；两个 SIC 槽位+下面的 WSIC 槽位可以通过拆卸滑道合并为一个 XSIC 槽位；两个 XSIC 槽位可以通过拆卸滑道合并为一个 EXSIC 槽位。AR2201-48FE-S 支持一个扩展卡槽位，不支持 SIC 卡槽位。**但槽位能合不能拆**，槽位合并后的新槽位号取两者中的较大者。

V200R002C00 及以后发布的版本通过特制的结构件，XSIC 槽位可以插一块 WSIC 卡，插在 XSIC 槽位的下半边，WSIC 卡的槽位号还是原 XSIC 槽位号。

设备名称		槽位分布图	槽位合并后的槽位分布图
AR2204-S	正面	NA	NA
	背面	4（SIC） 3（SIC） 2（SIC） 1（SIC） NA NA	2个SIC槽位合并为1个WSIC槽位 4（WSIC） 2（WSIC） NA NA
AR2220-S	正面	NA	NA
	背面	4（SIC） 3（SIC） 2（SIC） 1（SIC） 6（WSIC） 5（WSIC）	2个SIC槽位合并为1个WSIC槽位 4（WSIC） 2（WSIC） 6（WSIC） 5（WSIC）
			2个WSIC槽位合并为1个XSIC槽位 6（XSIC） 5（XSIC）

图 1-19　AR2204-S 和 AR2220-S 槽位分布图

设备名称		槽位分布图	槽位合并后的槽位分布图
AR2240-S	正面	10（电源） 9（电源） 风扇框 11（主控）	NA
	背面	4（SIC） 3（SIC） 2（SIC） 1（SIC） 6（WSIC） 5（WSIC） 8（XSIC） 7（XSIC）	2个SIC槽位合并为1个WSIC槽位 4（WSIC） 2（WSIC） 6（WSIC） 5（WSIC） 8（XSIC） 7（XSIC）
			2个WSIC槽位合并为1个XSIC槽位 6（XSIC） 5（XSIC） 8（XSIC） 7（XSIC）
			2个XSIC槽位合并为1个EXSIC槽位 6（XSIC） 5（XSIC） 8（EXSIC）

图 1-20　AR2240-S 槽位分布图

AR2220-S 系列各机型设备的槽位可以进行合并操作。

① AR2204-S 可以将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽

位 4。

② AR2220-S 可以将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽位 4；将新槽位 2 和槽位 5 合并为新槽位 5；将新槽位 4 和槽位 6 合并为新槽位 6。

③ AR2240-S 可以将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽位 4；将新槽位 2 和槽位 5 合并为新槽位 5；将新槽位 4 和槽位 6 合并为新槽位 6；将槽位 7 和槽位 8 合并为新槽位 8。

1.3.9　AR2200-S 系列路由器指示灯

AR2200-S 系列路由器的指示灯与前面介绍的 AR2200 系列一样，也在正面板和背面板上都有，但不同机型的指示灯状态及含义有所区别，具体对照关系如表 1-49 和表 1-50 所示。

表 1-49　AR2200-S 系列设备正面板指示灯

机型	指示灯
AR2201-48FE-S	其正面板指示灯如下图所示，指示灯及状态说明如表 1-51 所示 8 11 6 7 2 1 5 10 9 3 4
AR2204-S AR2220-S	AR2204-S 比 AR2220-S 面板正面多一个 RPS 指示灯，其他指示灯一样。下图是 AR2204-S 的正面板指示灯，指示灯及状态说明如表 1-52 所示 10 2 3 4 5 6 7 8 9 1 11
AR2240-S	AR2240-S 正面面板没有独立的指示灯，AR2240-S 面板上的指示灯全部是插在其槽位上各模块自身的指示灯。SRU40 主控板指示灯说明参见表 1-45

表 1-50　AR2200-S 系列设备背面板指示灯

机型	指示灯
AR2201-48FE-S	其背面板指示灯如下图所示，指示灯及状态说明参见表 1-51 对应序号指示灯 13 12
AR2204-S AR2220-S AR2240-S	AR2204-S、AR2220-S 和 AR2240-S 背面面板上没有独立的指示灯，面板上的指示灯全部是插在其槽位上各单板自身的指示灯，请参见产品手册中各业务单板的“指示灯说明”

表 1-51 AR2201-48FE-S 面板指示灯及状态说明

指示灯序号	指示灯	颜色	指示灯状态及含义
1	SYS	绿色	• 慢闪：表明系统处于正常运行状态 • 快闪：表明系统处于上电加载或者复位启动状态
		红色	常亮：表明单板有影响业务且无法自动恢复的故障，需要人工干预
		常灭	红灯、绿灯均不亮，表明软件未运行或处于复位状态
2	EN（CON/AUX 端口）	绿色	常亮：表明当前是 CON/AUX 端口使能
			常灭：表明当前不是 CON/AUX 端口使能
3	EN（SFP 光口）	绿色	• 常亮：表明 SFP 光口已经连通 • 闪烁：表明 SFP 光口有数据收发 • 常灭：表明 SFP 光口无链接
4	ACT（USB）	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行中
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，USB 接口故障或者指示灯故障
5	EN（MiniUSB 端口）	绿色	• 常亮：表明当前是 MiniUSB 端口使能 • 常灭：表明当前不是 MiniUSB 端口使能
6 和 7	GE 端口：绿灯为 LINK，黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
8	PWR	绿色	AR 内部电源供电正常
		常灭	设备未上电
9	RPS	绿色	常亮：RPS 电源在位
		黄色	常亮：RPS 电源已连接但状态异常
			闪烁：RPS 电源正在给设备供电
		常灭	RPS 电源未连接
10	WAN	绿色	常亮：WAN 处于连接/激活状态
			常灭：WAN 处于未连接/未激活状态
11	48FE 端口	绿色	常亮：表明 FE 端口已经连通
			闪烁：表明 FE 端口有数据传送
			常灭：表明 FE 端口无链接
12 和 13	扩展槽位指示灯： • 上面为 LINK，绿色 • 下面为 ACT，黄色	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发

表 1-52　**AR2204-S 正面板指示灯及状态说明**

指示灯序号	指示灯	颜色	指示灯状态及含义
1	SYS	绿色	● 慢闪：表明系统处于正常运行状态 ● 快闪：表明系统处于上电加载或者复位启动状态
		红色	常亮：表明单板有影响业务且无法自动恢复的故障，需要人工干预
		常灭	红灯、绿灯均不亮，表明软件未运行或处于复位状态
2	MiniSD 卡指示灯	绿色	常亮：表明链路已经连通
			闪烁：表明有数据收发
			常灭：表明无卡
3 和 4	SFP 端口： ● 上面为 LINK，绿色 ● 下面为 ACT，黄色	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
5 和 6	GE 端口：绿灯为 LINK，黄灯为 ACT	绿色	LINK 灯常亮：表明链路已经连通
			LINK 灯常灭：表明链路无链接
		黄色	ACT 灯闪烁：表明有数据收发
			ACT 灯常灭：表明无数据收发
7	ACT（USB）	红绿双色	绿色常亮：表明 U 盘开局正确完成
			绿色闪烁：表明 U 盘开局正在进行
			红色常亮：表明 U 盘开局失败
			常灭：表明未插开局 U 盘，USB 接口故障或者指示灯故障
8	EN（MiniUSB 端口）	绿色	常亮：表明当前是 MiniUSB 端口使能
			常灭：表明当前不是 MiniUSB 端口使能
9	EN（CON/AUX 端口）	绿色	常亮：表明当前是 CON/AUX 端口使能
			常灭：表明当前不是 CON/AUX 端口使能
10	PWR	绿色	AR 内部电源供电正常
		红色	AR 内部电源供电异常
		常灭	设备未上电
11	RPS	红绿双色	绿色常亮：RPS 电源在位
			黄色常亮：RPS 电源已连接但状态异常
			黄色闪烁：RPS 电源正在给设备供电
			常灭：RPS 电源未连接

1.3.10　AR3200 系列产品外观及配置规格

AR3200 系列目前仅一款机型：AR3260。它的正面外观如图 1-21 所示，各部件说明如下。

- 1——电源模块槽位 1：支持 2.2 A/350 W 交流电源模块、2.3 A/350 W 直流电源模块，但交流/直流电源模块不能混插。
- 2——电源模块槽位 2：支持的电源模块说明同上“电源模块槽位 1”。

- 3——多功能插槽槽位 1：支持插入电源模块，还通过拆卸两个多功能插槽中间的滑道，支持插入 SRU 主控板。
- 4——多功能插槽槽位 2：说明同上“多功能插槽槽位 1”。
- 5——风扇模块槽位。
- 6——SRU 主控板槽位。

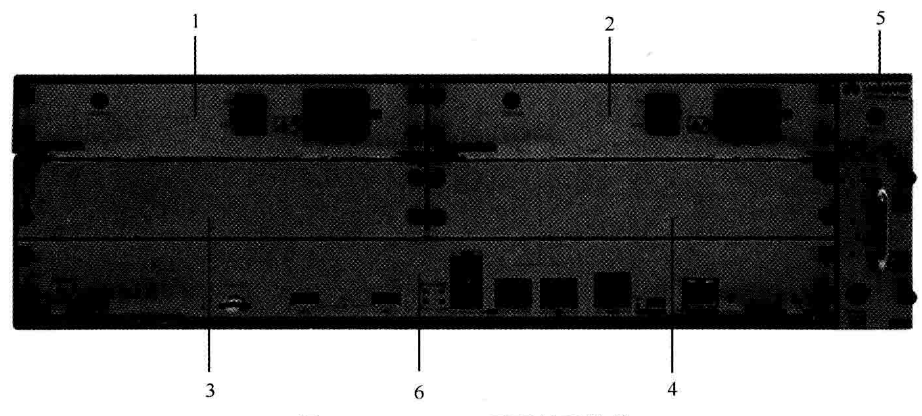


图 1-21　AR3260 正面外观结构

AR3260 背面外观结构如图 1-22 所示，各部件说明如下。

- 1——SIC 槽位：支持 4 个 SIC 槽位。
- 2——风扇模块槽位。
- 3——WSIC 槽位：支持两个 WSIC 槽位。
- 4——XSIC 槽位：支持 4 个 XSIC 槽位。

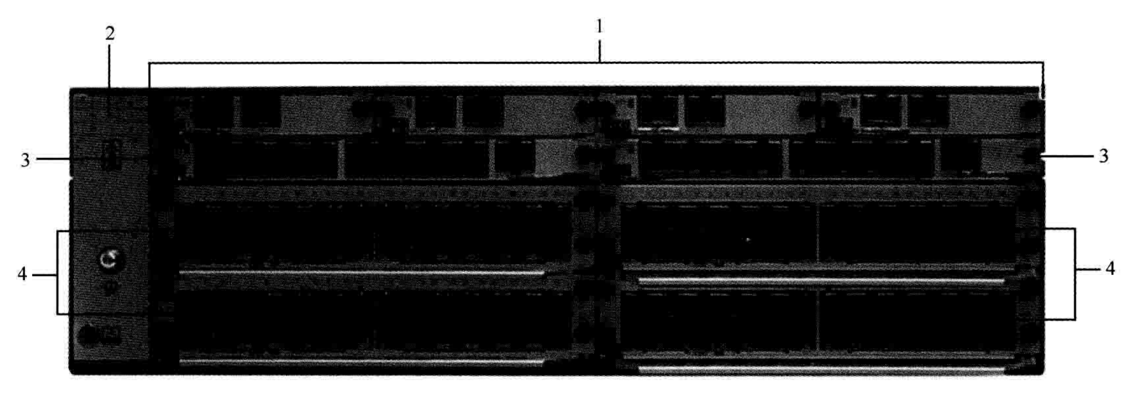


图 1-22　AR3260 背面外观结构

说明　AR3260 的槽位分布如图 1-23 所示。两个 SIC 槽位可以通过拆卸滑道合并为一个 WSIC 槽位；两个 SIC 槽位+下面的 WSIC 槽位可以通过拆卸滑道合并为一个 XSIC 槽位；两个 XSIC 槽位可以通过拆卸滑道合并为一个 EXSIC 槽位。MFS（Multiple Function Slot，多功能插槽）支持插入电源模块或者 SRU 主控板，当插入 SRU 主控板时，需要拆卸两个多功能插槽中间的滑道。**但槽位能合不能拆**，槽位合并后的新槽位号取两者中的较大者。

从 V200R002C00 版本开始，XSIC 槽位可以插一块 WSIC 卡，插在 XSIC 槽位的下半边，WSIC 卡的槽位号还是原 XSIC 槽位号。

AR3260 的槽位可以进行合并操作。

将槽位 1 和槽位 2 合并为新槽位 2；将槽位 3 和槽位 4 合并为新槽位 4；将新槽位 2 和槽位 5 合并为新槽位 5；将新槽位 4 和槽位 6 合并为新槽位 6；将槽位 7 和槽位 8 合并为新槽位 8；将槽位 9 和槽位 10 合并为新槽位 10；将槽位 13 和槽位 14 可以合并为新槽位 14，作为预留双主控升级能力的备用主控板槽位。

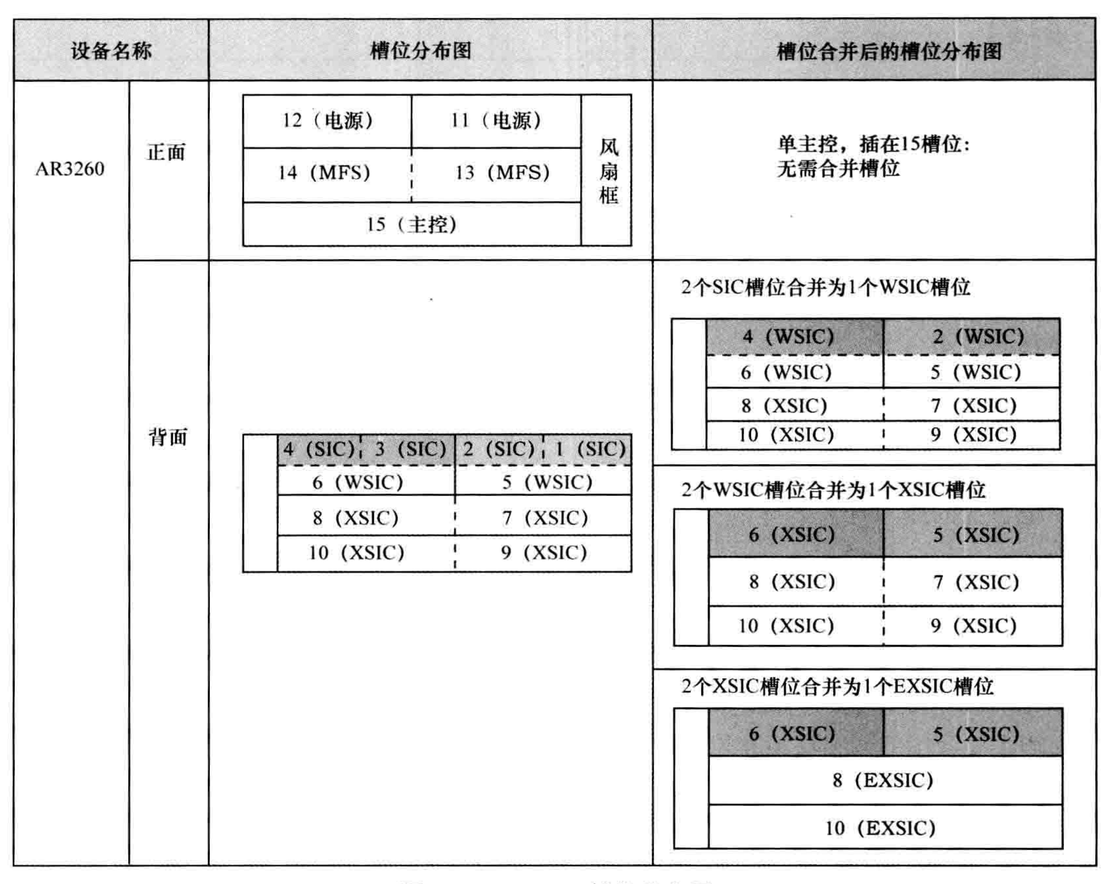


图 1-23　AR3260 槽位分布图

AR 3260 的基本配置规格如表 1-53 所示（以官网最新发布为准）。

表 1-53　AR 3260 基本配置规格

处理器	• 配置 SRU40：8 核 600 MHz • 配置 SRU60：8 核 600 MHz • 配置 SRU80：12 核 750 MHz
转发性能	5 Mpps～40 Mpps
带业务转发性能	600 Mbit/s～4.5 Gbit/s
整机交换容量	160 Gbit/s
每槽位交换容量	SIC 插槽 2 Gbit/s；WSIC 插槽 5 Gbit/s；XSIC 和 EXSIC 插槽 20 Gbit/s

（续表）

固定以太网路由端口	3×GE (2×Combo) /4×GE Combo/4×GE Combo+ 2×10GE
SIC 插槽	4
WSIC 插槽（缺省/最大）	2/4
XSIC 插槽（缺省/最大）	4/6
EXSIC 插槽	1
DSP 插槽	0/3
USB2.0 端口	2
Mini-USB 控制台端口	1
串行辅助/控制台端口	1
内存容量	2 GB/4 GB
Flash（缺省/最大）	2 GB/4 GB

1.3.11 AR3200 系列路由器指示灯

因为目前 AR3200 系列只有 AR 3260 这一款机型，所以在此仅介绍这一机型的指示灯及状态说明。

AR3260 正面板没有独立的指示灯，AR3260 面板上的指示灯全部是插在其槽位上各模块自身的指示灯，具体参见表 1-45 中所列出的 SRU 主控板指示灯。

AR3260 背面板也没有独立的指示灯，AR3260 面板上的指示灯全部是插在其槽位上各单板自身的指示灯，具体请参见产品手册中的各业务单板的“指示灯和接口说明”。

1.3.12 AR1200/1200-S/2200/2200-S/3200 系列路由器基本配置和性能综合比较

AR1200/1200-S/2200/2200-S/3200 系列都是模块化结构路由器，其主要应用也存在许多相同或相似之处。它们之间的主要区别在配置规格、主要功能和性能上，这也决定了它们主要应用的网络环境和位置的不同。在进行 AR G3 系列路由器选型时要特别注意。

AR1200/1200-S/2200/2200-S/3200 系列在基本配置和性能上的区别如表 1-54 所示（以官网最新发布为准）。

表 1-54 AR1200/1200-S/2200/2200-S/3200 系列路由器基本配置与性能综合比较

规格名称	AR1200	AR1200-S	AR2200	AR2200-S	AR3200
处理器	双核 500 MHz		双核 533 MHz 双核 800 MHz 四核 600 MHz SRU40：8 核 600 MHz SRU60：8 核 600 MHz SRU80：12 核 750 MHz	双核 533 MHz 双核 800 MHz 四核 600 MHz 八核 600 MHz	SRU40：8 核 600 MHz SRU60：8 核 600 MHz SRU80：12 核 750 MHz
转发性能	450 kpps，AR1200F 为 1.5 Mpps		350 kpps～20 Mpps	350 kpps～2 Mpps	5 Mpps～40 Mpps
带业务转发性能	200 Mbit/s，AR1200F 为 400 Mbit/s		200 Mbit/s～4.5 Gbit/s	200 Mbit/s～600 Mbit/s	600 Mbit/s～4.5 Gbit/s
整机交换容量	8 Gbit/s		10 Gbit/s～80 Gbit/s		160 Gbit/s

（续表）

<table>
<tr><td>固定以太网路由端口</td><td colspan="2">2×GE，AR1200F 为 2×GE (1×Combo)</td><td colspan="2">2～4×GE (1～2×Combo)</td><td>3×GE (2×Combo)/4×GE Combo/4×GE Combo+2×10 GE</td></tr>
<tr><td>固定以太网交换端口</td><td colspan="2">大部分机型：8×FE</td><td colspan="3">—</td></tr>
<tr><td>SIC 插槽</td><td colspan="2">2</td><td colspan="2">大部分机型支持 4 个 SIC 插槽</td><td>4</td></tr>
<tr><td>WSIC 插槽（缺省/最大）</td><td colspan="2">0/1</td><td colspan="2">大部分机型：2/4，小部分机型：0/2</td><td>2/4</td></tr>
<tr><td>XSIC 插槽（缺省/最大）</td><td colspan="2">—</td><td colspan="2">大部分机型：0/2，小部分机型：2/4 或 0</td><td>4/6</td></tr>
<tr><td>EXSIC 插槽（与 XSIC 共享插槽）</td><td colspan="2">—</td><td colspan="2">大部分机型无 EXSIC 插槽，小部分机型有 1 个</td><td>1</td></tr>
<tr><td>DSP 插槽</td><td>部分支持 32 路语音</td><td>—</td><td colspan="2">支持 0～3 个 DSP 插槽</td><td>0/3</td></tr>
<tr><td>WIFI</td><td colspan="2">部分机型支持 802.11b/g/n</td><td colspan="3">—</td></tr>
<tr><td>USB2.0 端口</td><td colspan="2">2，AR1200F 为一个 USB 端口</td><td colspan="2">大部分机型为两个，小部分机型为一个</td><td>2</td></tr>
<tr><td>Mini-USB 控制台端口</td><td colspan="5">1</td></tr>
<tr><td>AUX/CON 端口</td><td colspan="5">1</td></tr>
<tr><td>内存容量</td><td colspan="2">512 MB</td><td colspan="2">512 MB～4 GB</td><td>2 GB/4 GB</td></tr>
<tr><td>Flash（缺省/最大）</td><td colspan="2">256 MB，AR1200F 为 512 MB</td><td>大部分机型 512 MB/4 GB，小部分机型 512 MB 或者 2 GB/4 GB</td><td>16 MB 或者 512 MB</td><td>2 GB/4 GB</td></tr>
</table>

1.3.13　AR1200/1200-S/2200/2200-S/3200 系列路由器的主要应用

AR1200/1200-S/2200/2200-S/3200 系列路由器在许多方面基本上一样，主要区别就是应用的网络场景和位置上的不同：AR1200/1200-S/2200/2200-S 应用于企业分支，AR3200 系列用于企业总部。这三个系列均有一些特殊的应用，具体将在下面的应用介绍中说明。

1. 丰富多样的广域网互联接入

AR1200/1200-S 系列企业路由器作为分支用户的出口路由器，支持广域网的各种灵活接入方式，可进行远程网络互联，如图 1-24 所示。单一设备就能满足专线、以太、xDSL、3G、WLAN 等多种接入需求，节约了部署运维成本。AR1220V、AR1220W 和 AR1220VW 的固定百兆以太口还支持 IEEE 802.3af 和 802.3at 标准的 PoE 功能，通过双绞线向远端下挂受电设备（如 IP Phone 等）供电。其中 802.3at 端口的输出功率在 30W 以上，能保证大功率受电设备的供电。

2. 高密度以太网接入

AR2200/2200-S/3200 系列企业路由器提供 24GE 以太接口卡，能实现大容量高密度

千兆接入的应用，方便网络运维，节省客户投资。

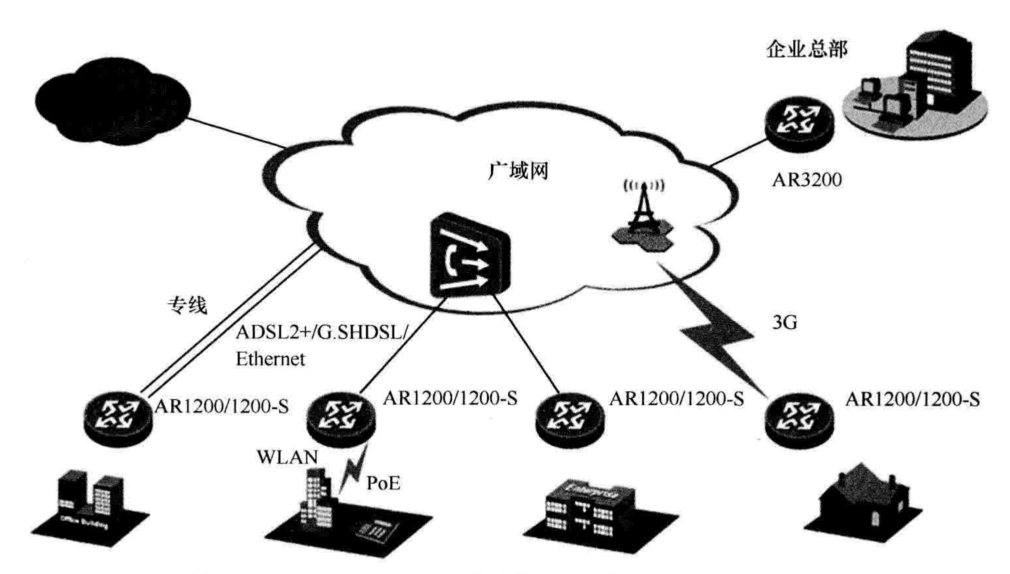


图 1-24 AR1200/1200-S 系列在广域网接入方面的典型应用

AR2201-48FE 和 AR2202-48FE、AR2201-48FE-S 和 AR2202-48FE-S 是 AR2200/2200-S 系列路由器中新一代的路由交换一体化产品，这四款设备上集成了 48 个百兆以太网端口和两个千兆以太网端口，在极大程度上满足了分支高密以太的接入要求。通过一体机可实现接入交换机、分支出口路由器合一的功能，降低客户采购成本。同时可减少设备故障点，降低网点的维护难度。

AR2200/2200-S 系列路由器的以太网接入典型网络结构如图 1-25 所示；AR3200 系列路由器的以太网接入典型网络结构如图 1-26 所示。

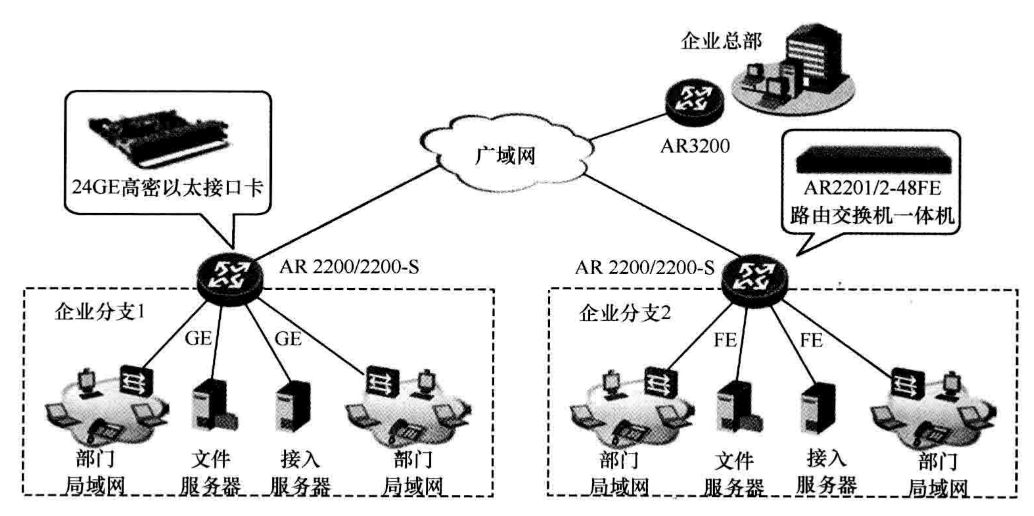


图 1-25 AR2200/2200-S 系列路由器的以太网接入典型网络结构

3．优质融合的语音服务

AR1200/1200-S/2200/2200-S/3200 系列企业路由器作为企业语音业务网关，可用作

IP PBX 和 SIP 接入网关。在 IP PBX 应用场景中，它们内置 PBX，可提供企业总机、IVR 语言导航、话单查询等语音通信业务，有效提升了企业形象，提高了企业内外的沟通效率。AR1200/1200-S/2200/2200-S 系列路由器可部署在企业分支，AR3200 系列可部署在企业总部，支持智能路由拨号功能，可以根据目的号码段智能选择出口链路，节省企业分支话费开支，典型应用网络结构如图 1-27 所示。

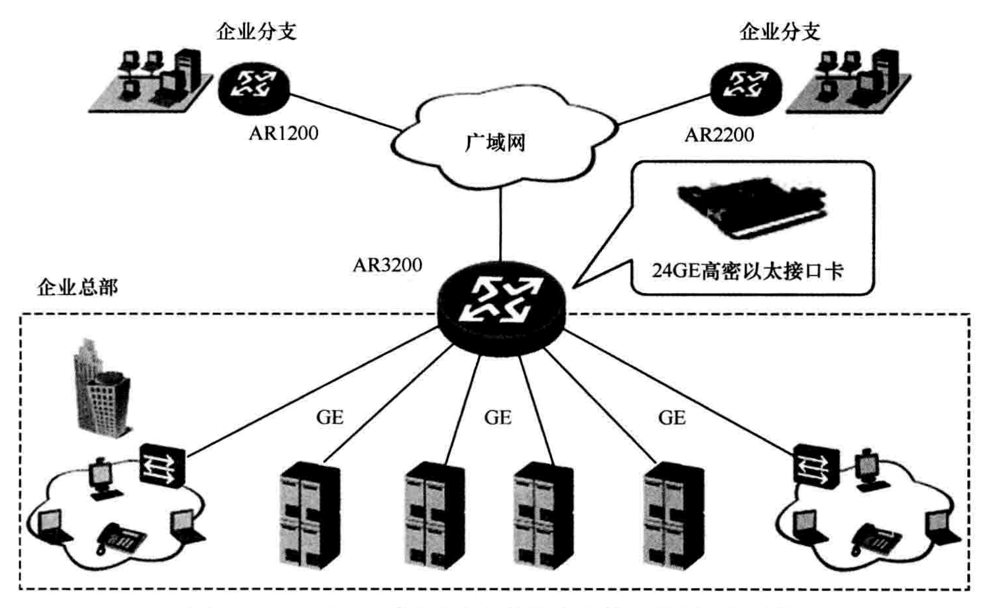


图 1-26　AR3200 系列路由器的以太网接入典型网络结构

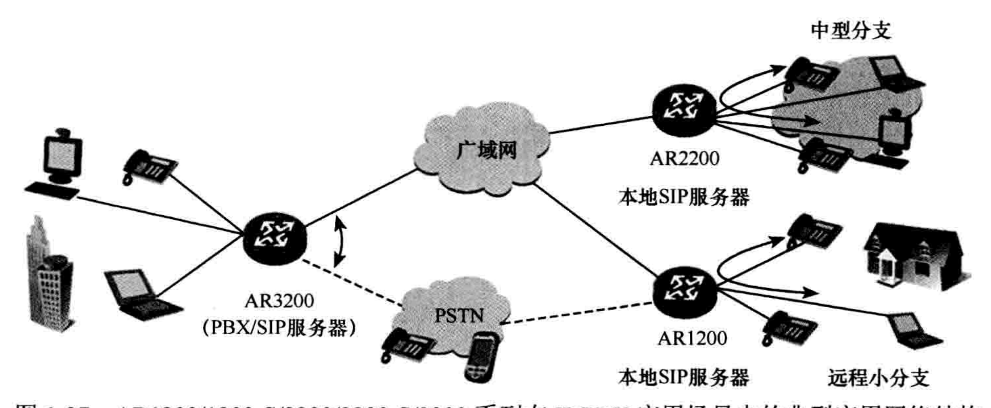


图 1-27　AR1200/1200-S/2200/2200-S/3200 系列在 IP PBX 应用场景中的典型应用网络结构

在 SIP 接入网关应用场景中，AR1200/1200-S/2200/2200-S/3200 系列企业路由器将传统语音、传真与现代 IP 业务有效融合。当运营商为企业部署语音时，AR1200/1200-S/2200/2200-S 系列可作为企业分支的 SIP 接入网关，AR3200 系列可作为企业总部的 SIP 接入网关，将普通语音电话信号转化为 VoIP 信号进行呼叫管理，典型网络结构如图 1-28 所示。上行与 IMS/NGN 网络互连，实现固话、手机、PC 等任意终端在任意时间的语音通信。

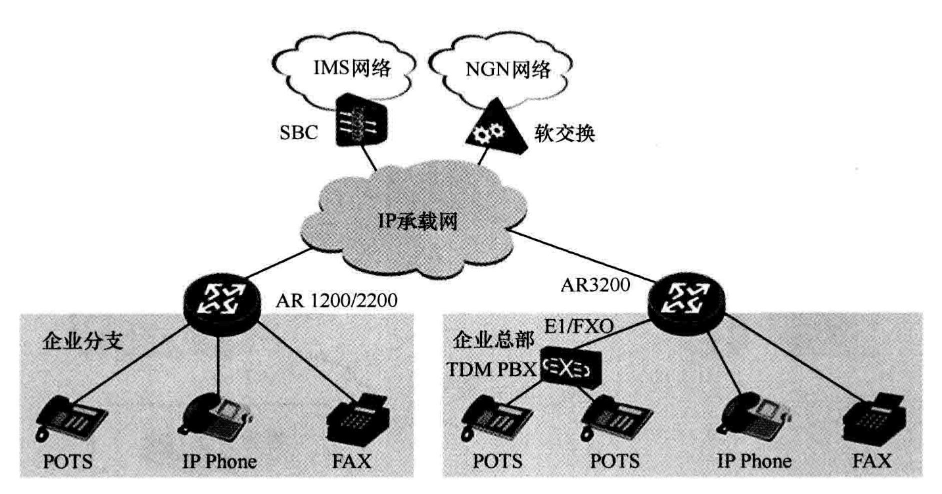


图 1-28　AR1200/1200-S/2200/2200-S/3200 系列在 SIP 接入网关应用场景中的典型应用网络结构

4. 灵活便捷的分支 3G 无线接入

AR1200/1200-S/2200/2200-S 系列企业路由器支持 3G 接入功能，支持 CDMA2000 EV-DO、WCDMA 的 3G 标准，满足了企业分支机构之间以及与总部间的无线互联需求，典型网络结构如图 1-29 所示。

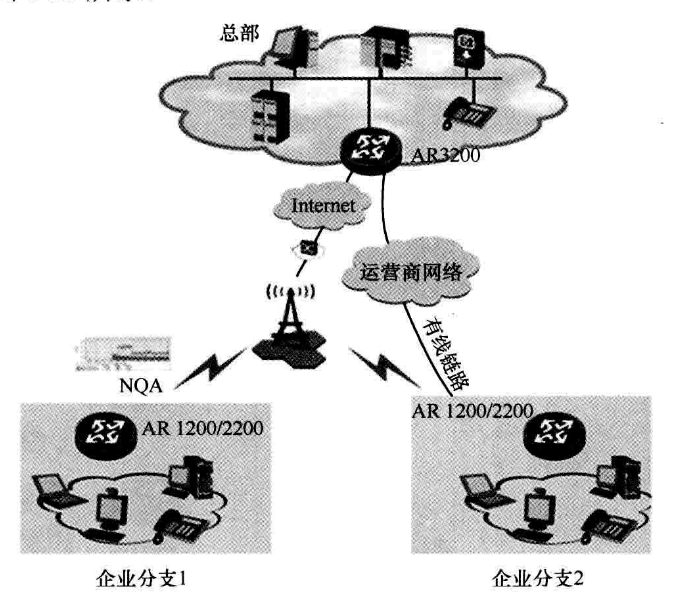


图 1-29　AR1200/1200-S/2200/2200-S 系列在 3G 无线接入方面的典型应用

采用 3G USB 数据卡接入方式，客户在 AR 上部署 3G 业务时，不占用设备的业务槽位，最大程度地保护了客户的投资。同时，3G 数据链路可以作为有线链路的备份链路，对 AR 上行的 xDSL、FE/GE、ISDN 等链路提供链路保护，有效提高网络的稳定性，降低网络建设成本。NQA 技术还可以实时监控 3G 链路质量，有效保证用户的 SLA。

5. 无线 AC 管理场景

AR1200/1200-S/2200/2200-S/3200 系列企业路由器集成了 AC 功能，可对无线局域网中的 AP 进行控制和管理。AR1200/1200-S/2200/2200-S 系列路由器可用于企业分支，

AR3200 系列路由器可用于企业总部，典型网络结构如图 1-30 所示。AR 支持丰富的认证方式和灵活的用户权限控制，能为 Wi-Fi 用户提供安全接入保证，同时集丰富的无线功能于一身，实现了对有线无线一体化网络的集中管理，满足了不同规模企业的建网要求。

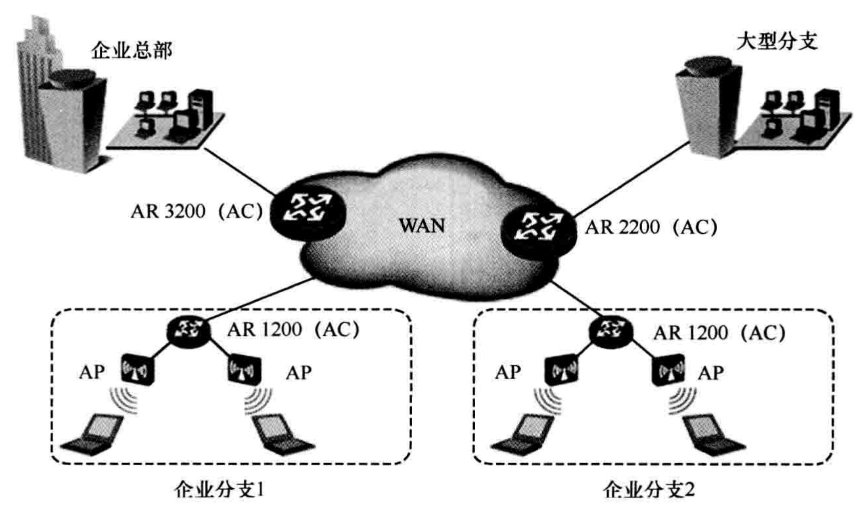


图 1-30　AR1200/1200-S/2200/2200-S/3200 系列在无线 AC 管理方面的典型应用

6. 丰富的企业分支 VPN 组网

AR1200/1200-S/2200/2200-S/3200 系列企业路由器提供了多种安全接入功能，满足了企业分支之间、企业分支与总部之间以及合作伙伴访问企业内部信息的需求，典型网络结构如图 1-31 所示。总部和分支机构建立隧道，包括 GRE VPN、IPSECVPN、DSVPN、SSL VPN、L2TP VPN 安全隧道，以实现数据的安全访问与传输，支持分支机构侧隧道的快速部署和认证等功能。通过远程隧道接入方式，合作伙伴可灵活访问企业内部资源，实现企业内资源的安全和共享。

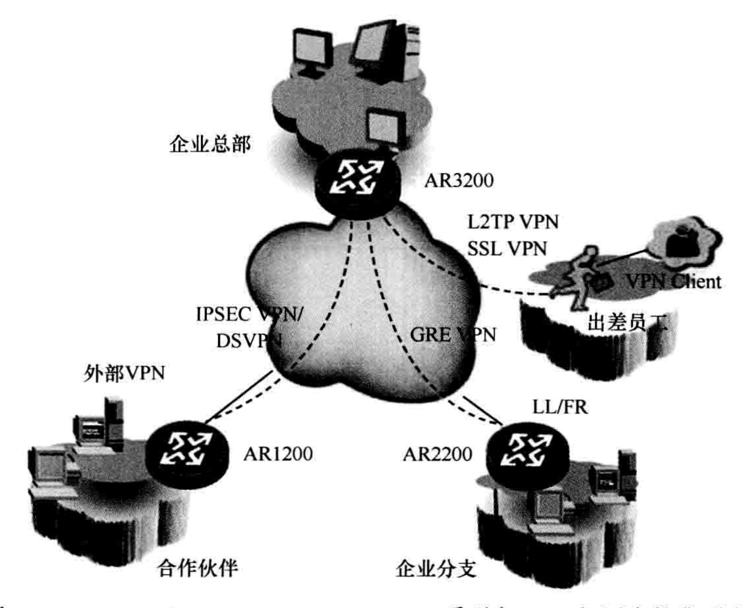


图 1-31　AR1200/1200-S/2200/2200-S/3200 系列在 VPN 组网中的典型应用

另外，AR3200系列路由器还可作为MPLS网络的PE设备被部署在企业总部和分支，不同业务之间通过MPLS L3 VPN隔离，以实现VPN业务的灵活部署、快速转发、安全传输，实现企业业务的虚拟化运营，典型网络结构如图1-32所示。

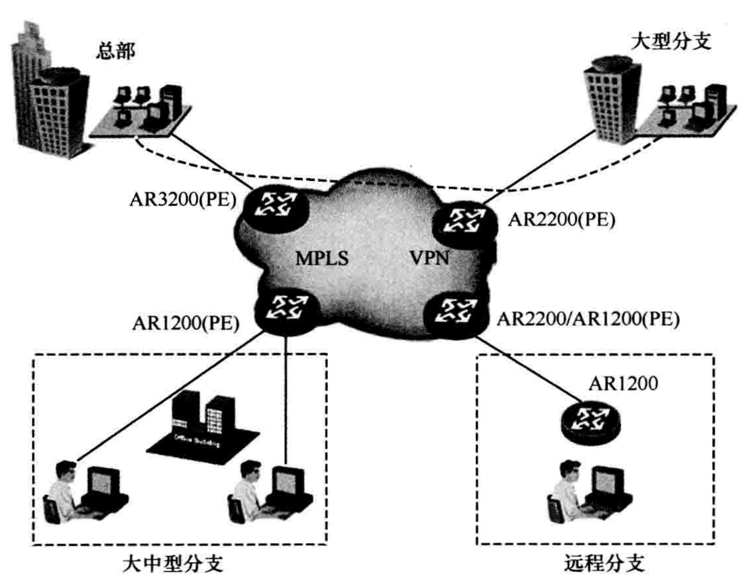


图1-32 AR3200系列在MPLS VPN组建方面的典型应用

7. 高密度E1汇聚分支接入

AR3200系列企业路由器支持丰富的接口类型，包括高密度E1、CPOS、POS等多款板卡，满足各个分支机构和总部间的汇聚接入要求，典型网络结构如图1-33所示。企业多个小型分支机构可通过E1链路上行连接至汇聚层路由器，通过其支持的高密E1板卡或者CPOS提供汇聚接入，然后通过POS上行到高端路由器连接核心网络。

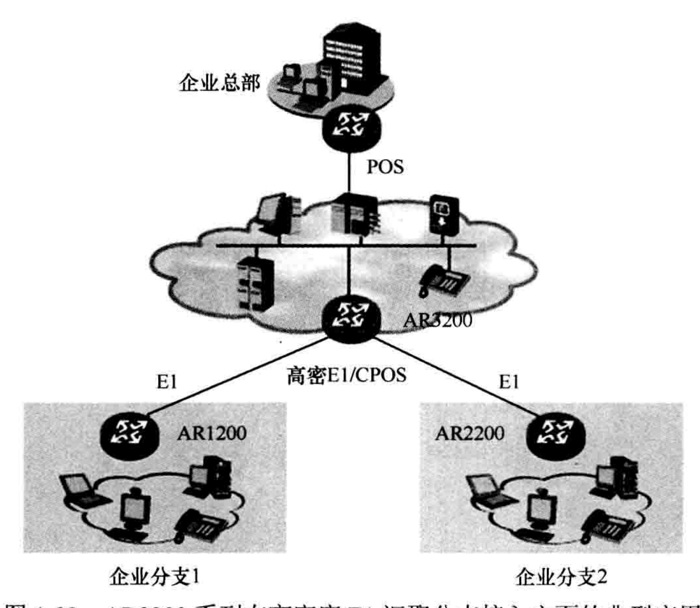


图1-33 AR3200系列在高密度E1汇聚分支接入方面的典型应用

1.4　NE 系列路由器

NetEngine（简称 NE）系列是华为公司面向网络骨干节点、汇聚节点、边缘节点的高端路由器产品。目前市场中主要应用的是 NE20E-S、NE40E 和 NE5000E 三个子系列。本节将简单介绍这几个系列产品的主要特点和基本特性。

1.4.1　NE20E-S 系列多业务路由器的主要特点

NE20E-S 系列多业务路由器是华为公司推出的高端路由器产品，主要应用于 IP 骨干网汇聚、中小企业网核心、园区网边缘、中小校园网接入等。

NE20E-S 系列路由器基于硬件的转发机制和无阻塞交换技术，采用华为公司自主研发的通用路由平台 VRP，具有电信级的可靠性、全线速的转发能力、完善的 QoS 管理机制、丰富的业务处理能力和良好的扩展性等特点。它可以灵活部署 L2VPN、L3VPN、组播、组播 VPN、MPLS TE（流量工程）、QoS 等，实现业务运营级的可靠承载。同时，NE20E-S 系列路由器全面支持 IPv6，可以实现 IPv4 到 IPv6 的平滑过渡。

目前 NE20E-S 系列主要包括 NE20E-S4，NE20E-S8 和 NE20E-S16 这三款不同配置规格的机型（如图 1-34 所示），分别支持 4 个、8 个和 16 个槽位，适应不同规模的网络组网需求。



图 1-34　NE20E-S 系列的三款机型

NE20E-S 系列路由器的主要特点如下。

1. 最新的 VRP 平台

NE20E-S 系列路由器采用最新的 VRP8 平台，采用 RDF（Resilient Distributed Framework，弹性分布式架构），通过相对分离的管理平面、业务平面、数据平面和控制平面，极大地提升了整个系统的灵活性、可靠性、可管理性、扩展性。

2. 领先的工业设计

NE20E-S 系列路由器采用业界领先的工业设计，其 220 mm 深的小巧机箱带来了最大 480 Gbit/s 的交换容量，适合各种空间布放条件；其抗高温低温的设计可以满足 −40℃～65℃的工作条件，非常适合条件恶劣的室外布放。另外，其功耗做到了低于业界水平。

3. 强大的路由和业务支持能力

NE20E-S 系列路由器具有强大的路由能力，支持超大路由表，提供 RIP、OSPF、IS-IS、BGP4 和多播路由等丰富的路由协议，支持明/密文认证，具备快速收敛功能，能保证在复杂的路由环境下安全稳定。

同时，NE20E-S 系列路由器具有强大的业务承载能力，根据组网需求可以同时部署 L2VPN、 L3VPN、MVPN；支持和 TE（Traffic Engineering，流量工程）同时部署；支持丰富的接入类型（E1、POS、cPOS、GE、10GE）；支持灵活 QinQ，支持 DHCP；还可提供 Netstream 等功能，适应传统的接入需求和新兴的业务需求，满足多业务融合丰富的承载需求；具有强大的可扩展组播能力，支持丰富的 IPv4/IPv6 组播协议，包括 PIM-SM/SSM、MLDv1/v2、IGMPv3，IGMPSnooping 等特性，可以灵活承载 IPTV 等视频业务，可以满足各种规模的组播业务的需求。

4. 全方位的可靠性解决方案

NE20E-S 系列路由器从多个层面提供可靠性保护，包括设备级、网络级、业务级可靠性，形成了面向整个网络的解决方案，完全满足电信级的可靠性需求，是构筑电信级业务的基石，达到 99.999%的系统可用性。具体表现如下。

① 设备级可靠：NE20E-S 系列路由器提供关键部件的冗余备份。关键组件支持热插拔与热备份、NSR（Non-Stop Routing，无中断路由）、NSF（Non-Stop Forwarding，无中断转发）等技术一起保障无中断业务运行。

② 网络级可靠：NE20E-S 系列路由器提供 IP/LDP/VPN/TE 快速重路由，Hot- Standby，IGP、BGP 以及组播路由快速收敛，VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议），TRUNK 链路分担备份，BFD 链路快速检测，MPLS/Ethernet/MPLS- TP OAM，保证整网稳定性，可以提供端到端 200 ms 保护倒换，业务无中断。

③ 业务级可靠：NE20E-S 系列路由器提供的 VPN FRR 和 E-VRRP 技术，VLL FRR 和 Ethernet OAM 技术以及 PW Redundancy 和 E-Trunk 技术，可以应用于 L3VPN 和 L2VPN 组网方案中，保证业务层面的冗余备份，使业务稳定可靠，不中断。

1.4.2 NE20E-S 系列多业务路由器的主要特性

NE20E-S 系列多业务路由器支持丰富的各种高端路由器特性，其三款机型的主要特性如表 1-55 所示。

表 1-55 NE20E-S 系列多业务路由器主要特性

特性	NE20E-S4	NE20E-S8	NE20E-S16
交换容量	240 Gbit/s	480 Gbit/s	480 Gbit/s
转发性能	180 Mpps	360 Mpps	360 Mpps
槽位数	4	8	16
接口类型	10GE-WAN/LAN、GE/FE、OC-3c/STM-1c POS、Channelized OC-3/STM-1 POS 和 E1/cE1		
二层特性	• 支持 IEEE802.1q、IEEE802.1p、IEEE 802.3ad、IEEE 802.1ab • 支持 STP/RSTP/MSTP、RRPP、VLAN Switch 和用户绑定		
IPv4/IPv6 路由协议	• 支持静态路由、RIP、OSPF、IS-IS、BGP 等 IPv4 路由协议 • 全面支持 IPv4 和 IPv6 双协议栈 • 支持丰富 IPv4 向 IPv6 的过渡技术：手工配置隧道、自动配置隧道、6to4 隧道、6PE • 支持 IPv6 静态路由，支持 BGP4/BGP4+、OSPFv3、ISISv6 等动态路由协议 • 支持 IPv6 邻居发现，PMTU 发现，TCP6，ping IPv6，tracert IPv6，socket IPv6、IPv6 策略路由		

（续表）

L2/L3 VPN	• 支持 LDP over TE、VPLS/H-VPLS、VPN 策略路由 • 支持 Martini 方式的 MPLS 二层 VPN • 支持 VLL/VPLS 接入 L3 VPN • 支持 MPLS/BGP 三层 VPN • 支持跨域 VPN
组播	支持 IGMP v1/v2/v3、IGMP Snooping、IPv6 组播、静态组播路由、PIM-SM/SSM、MBGP，支持同时部署组播和 TE
QoS	支持 WRED、五级 H-QoS、VLL/PWE3、接入 QoS 控制和用户位置报告
可靠性	• 支持 BGP/BGP4+/ISIS/ISIS6/OSPF/OSPFv3/PIM/IGMP/LDP/RSVP-TE/L3VPN NSR • 支持 BGP/IS-IS/OSPF GR/LDP GR/RSVP GR/NSF • 支持 VLL（虚拟租用线路）/VPLS（虚拟专用局域网业务）/L3VPN GR/NSF • 支持 BGP/IGP/组播快速收敛 • 支持 IP/LDP FRR、TE FRR、VPN FRR 和 VLL FRR • 支持静态路由、IS-IS、RSVP、LDP、TE、LSP、PW、OSPF、BGP、VRRP、PIM 的 BFD 功能 • 支持以太网 OAM（L2 LSA、802.1ag 和 802.1ah）、Y.1731、PWE3 端到端保护

1.4.3 NE40E 系列全业务路由器的主要特点

NE40E 系列全业务路由器是华为公司推出的高端网络产品，主要应用在企业广域网核心节点、大型企业接入节点、园区互联/汇聚节点以及其他各种大型 IDC 网络的边缘位置，与下面将要介绍的 NE5000E 骨干路由器、前面介绍的 NE20E-S 汇聚路由器产品配合组网，形成结构完整、层次清晰的 IP 网络解决方案。

NE40E 基于 CLOS（Common Lisp Object System，公共 LISP 对象系统）分布式多级交换架构，采用了分布式的硬件转发和无阻塞交换技术，具有良好的线速转发性能，优异的扩展能力，完善的 QoS 机制和强大的业务处理能力。NE40E 基于最新的可扩展 400 Gbit/s 平台，可实现到 400 Gbit/s/槽位的平滑扩展，且兼容现网所有线卡，最大限度地保护了客户的投资。NE40E 具有支持虚拟化的能力，可将多台设备虚拟成一台。

NE40E 具有强大的汇聚接入能力，凭借丰富的特性支持，可以灵活部署 L2VPN、L3VPN、组播、组播 VPN、MPLS TE、QoS 等，实现业务的可靠承载；同时，NE40E 全面支持 IPv6，可以实现 IPv4 到 IPv6 的平滑过渡。因此，NE40E 可以灵活应用在 IP/MPLS 网络的边缘、核心，可以简化网络结构，提供丰富的业务类型和可靠的服务质量，是 IP/MPLS 承载网向宽带化、安全化、业务化、智能化发展的重要源动力。

目前 NE40E 系列主要包括 NE40E-X3、NE40E-X8 和 NE40E-X16 这三款不同配置规格的机型（如图 1-35 所示），分别支持 3 个、8 个和 16 个业务线路板槽位，适应不同规模的网络组网需求。

NE40E 系列全业务路由器具有以下主要特点。

1. 领先的 400 Gbit/s 平台

NE40E 系列路由器基于 400 Gbit/s 平台，每槽位可以平滑扩容到 400 Gbit/s 带宽，提供 100 Gbit/s 单板，实现大容量业务承载，满足未来带宽增长需求。同时，NE40E 系列基于现有 VRP 软件平台，完全兼容现网所有线卡，最大限度地保护了客户的投资。整机采用高密度端口、紧凑性设计，可以有效地节省空间。

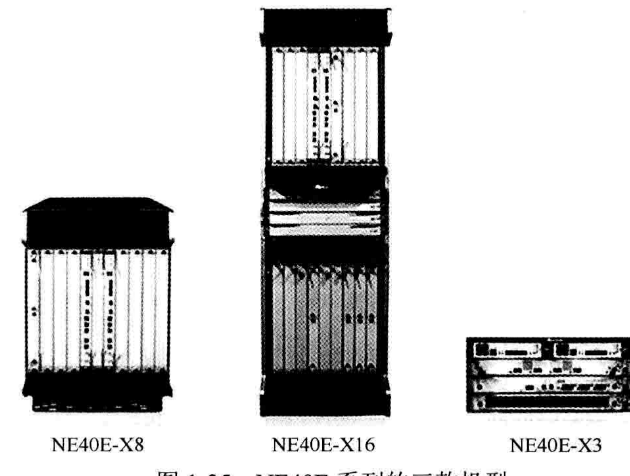


图 1-35 NE40E 系列的三款机型

2. 绿色的设计理念

NE40E 系列路由器整机采用完全绿色的设计，更加环保节能。NE40E 采用业界领先的冷却和节能系统，包括先进的风道设计、最优的散热设计、智能化风扇设计和分区供电设计，可以做到温度自动感知和自动调节，极大地提高了电源的利用率。采用低功耗芯片设计，使 NE40E 在绿色节能方面具有更明显的优势。

3. 强大的路由和业务支持能力

NE40E 系列路由器具有强大的路由能力，支持超大路由表，提供 RIP、OSPF、IS-IS、BGP4 和多播路由等丰富的路由协议，支持明/密文认证，具备快速收敛功能，保证在复杂路由环境下安全稳定。

NE40E 系列路由器具有强大的业务承载能力，根据组网需求可以同时部署 L2VPN、L3VPN、MVPN；支持和 TE（Traffic Engineering）同时部署；支持丰富的接入类型（ATM、IMA E1、TDM、POS、Ethernet）；支持灵活 QinQ，支持 DHCP/IpoE；还可提供 IPSec、NAT、GRE 等功能，适应传统的接入需求和新兴的业务需求，满足多业务融合丰富的承载需求；具有强大的可扩展组播能力，支持丰富的 IPv4/IPv6 组播协议，包括 PIM-SM/DM/SSM、MLDv1/v2、IGMPv3、组播 CAC（Call Admission Control，呼叫许可控制）、IGMP Snooping 等特性，可以灵活承载 IPTV 等视频业务，满足各种规模的组播业务的需求。

NE40E 系列路由器还集成了视频缓存的功能，提供完美的 IPTV 体验。通过视频体验增强卡（VSUF-10）提供快速频道切换（FCC）、丢包重传（RET）和实时的视频监控，改善了用户体验，优化了网络管理。另外，NE40E 系列路由器通过存储来换取宝贵的带宽资源，降低了全网的 TCO。

4. 支持 IPv6 兼容方案

NE40E 系列路由器支持丰富的 IPv6 特性，包括 IPv6 专线接入、双栈、隧道及翻译。NE40E 支持下一跳分离技术优化 IPv6 路由收敛时间，提供大容量 IPv6 FIB，增强了网络可扩展性。NE40E 提供了完善的 IPv4-IPv6 解决方案，满足以上各种演进场景向 IPv6 过渡的需求。

5. 全方位的可靠性解决方案

NE40E 从多个层面提供可靠性保护，包括设备级、网络级、业务级可靠性，形成了面向整个网络的解决方案，完全满足电信级的可靠性需求，是构筑电信级业务的基石，达到 99.999%的系统可用性。这方面的具体描述参见 1.4.1 小节 NE20E-S 系列路由器中的此特点。

6. 完善的 QoS 机制

NE40E 系列路由器提供高品质的 QoS 能力，具体先进的队列调度算法、拥塞控制算法，能够对数据流实现多级的精确调度，从而满足不同用户、不同业务等级的服务质量要求。其分布式 QoS 引擎最大能够提供 200 ms 的包缓存能力，可解决广域网 IP 突发流量造成的丢包问题。

NE40E 系列路由器具备完善的 QoS 调度机制：支持面向接入侧的 H-QoS 五级调度机制，其多样化、差异化满足了接入侧不同层次用户的业务需求；支持面向网络侧的 MPLS H-QoS 功能，支持在网络侧部署 QoS 功能，实现了 MPLS VPN、VLL 和 PWE3 的 QoS 能力；支持基于 TE 的 MPLS DS-TE，实现 MPLS TE 与 DiffServ 模型的结合，支持 8CT（Class Type），支持 MAM（Maximum Allocation Model，最大分配模型）和 RDM（Russian Dolls Model，俄罗斯多尔模型）两种带宽约束模型，有效地保证网络承载的 QoS 需求。

1.4.4 NE40E 系列全业务路由器的主要特性

NE40E 系列是全业务路由器，所支持的路由器业务功能和性能较前面介绍的 NE20E-S 还要强大，其三款机型的具体特性表现如表 1-56 所示（以官网最新发布为准）。

表 1-56 NE40E 系列路由器主要特性

特性	NE40E-X16	NE40E-X8	NE40E-X3
交换容量	50.32 Tbit/s	25.16 Tbit/s	1.08 Tbit/s
转发性能	11520 Mpps	5760 Mpps	540 Mpps
槽位数	22 个，其中 16 个业务线路板槽位，2 个主控板槽位，4 个交换网板槽位	11 个，其中 8 个业务线路板槽位，2 个路由交换板槽位，1 个交换网板槽位	5 个，其中 3 个业务线路板槽位，2 个主控板槽位
接口类型	100GE/40GE、GE/FE、C-192c/STM-64c POS、OC-12c/STM-4c POS、Channelized OC-3/STM-1、OC-12c/STM-4c ATM、CE1/CT1		10GE-LAN/WAN、OC-768c/STM-256c POS、OC-48c/STM-16c POS、OC-3c/STM-1c POS、OC-3c/STM-1c ATM、E3/CT3、E1/T1
IPv4	支持 Static routing 、RIP、OSPF、IS-IS、BGP-4 等路由协议，所有端口在路由振荡等复杂路由环境下线速转发		
IPv6	• 支持丰富 IPv4 向 IPv6 的过渡技术：手工配置隧道、自动配置隧道、6to4 隧道，GRE 隧道，ISATAP 隧道等 • 支持 IPv4 over IPv6 隧道和 6PE • 支持 IPv6 静态路由，支持 BGP4/BGP4+、RIPng、OSPFv3、ISISv6 等动态路由协议 • 支持 IPv6 邻居发现，PMTU 发现，TCP6，ping IPv6，traceroute IPv6，socket IPv6，静态 IPv6 DNS • IPv6 DNS 服务器，TFTP IPv6 client，IPv6 策略路由 • 支持 ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等 • 支持 CGN、L2NAT、NAT444、DS-LITE、NAT64		

（续表）

MPLS	支持 MPLS TE，支持 MPLS/BGP VPN，符合 RFC2547bis 协议；支持三种跨域实现方式；支持与 Internet 业务集成；支持基于 Martini、Kompella 方式的 MPLS L2 VPN，支持 VPLS/VLL 等多种二层 VPN 技术，支持异种介质互联；支持组播 VPN；支持 MPLS-TP
二层特性	支持 IEEE 802.1Q，IEEE 802.1ad，IEEE 802.1D，IEEE 802.1w，IEEE 802.1s 等相关协议，支持 VLAN 聚合（Super VLAN）、支持基于 MAC 地址和端口的过滤列表、支持 1 483 B
可靠性	提供 IP/LDP/VPN/TE/VLL 快速重路由，支持 IP/TE 自动重路由，IGP/BGP/组播路由快速收敛、虚拟路由冗余协议（VRRP）、快速环网保护协议（RRPP）、IP TRUNK 链路分担备份、BFD 快速检测、MPLS/Ethernet OAM、Y.1731、路由协议/端口/VLAN Damping 等保护机制。支持 PW redundancy、E-Trunk、E-APS、E-STP。提供软件热补丁技术，实现软件平滑升级；采用无源背板设计；路由处理模块、交换网、电源等关键部件冗余备份，整机没有单点故障；支持基于状态的热备份切换，支持平滑重启（GR）、支持不中断转发（NSF），支持不中断路由（NSR），支持 ISSU，所有组件可热拔插
QoS	完善的 HQoS 机制。每线路板可提供先进调度和拥塞避免技术；提供精确的流量监管和流量整形功能；提供定义复杂规则的功能，支持流细粒度鉴别。支持 MPLS HQoS，全面保证 MPLS VPN、VLL 和 PWE3 的 QoS。提供基于 DiffServ 和 MPLS TE 的 DS-TE，支持 8CT（Class Type），支持面向 TE 隧道的 QoS
组播	支持 IGMP v1/v2/v3 协议，支持静态组播配置，支持 PIM-DM/SM/SSM、MSDP、MBGP 组播路由协议；支持组播 CAC；支持多个组播协议间的互操作性；支持组播策略处理，包括组播路由协议和组播转发的策略处理，支持组播 QoS，支持 IPOE 接入用户的组播复制；提供交换网和线路板两级组播复制功能，达到最优的组播效能
安全	支持 ACL 报文过滤，支持 URPF，支持 GTSM，支持 DHCP Snooping，支持防 ARP 攻击、防 DOS 攻击，支持 MAC 地址限制、MAC 与 IP 绑定；支持 SSH、SSH v2，支持 NetStream，支持 IPSec

1.4.5 NE5000E 集群路由器的主要特点

NE5000E 集群路由器是华为公司面向互联网骨干节点、城域网核心节点、数据互联中心节点以及 Internet 承载节点推出的超级核心路由器产品。NE5000E 采用华为自主研发的 Solar 系列芯片、先进的光背板设计和分布式可扩展软件平台，可提供海量交换容量和超高转发性能，全面满足新一代互联网对带宽性能、服务质量、业务能力的需要。

NE5000E（如图 1-36 所示）在硬件上包括两部分，CCC（Cluster Central Chassis，集群中央框）和 CLC（Cluster Line Chassis，集群线路框）。CLC 用于用户和业务的高速接入，可工作在单框模式和多框集群模式，CCC 用于集群系统，主要用于连接各线卡框的控制平面和数据平面，使多台 CLC 在逻辑上连接，实现系统的统一管理和控制。

NE5000E 路由器的主要特点如下。

1. 每槽位 400 Gbit/s 平台

2008 年 4 月，华为业界首家推出 NE5000E 二拖八集群系统，支持每槽位 40 Gbit/s 容量，领跑因特网 10 Tbit/s 时代；通过采用 100 Gbit/s 技术，二拖八集群系统容量达到 25 TB，可满足运营部署超大带宽业务的需要。NE5000E 采用先进的无阻塞交换网络架构，具有 400 Gbit/s 硬件平台，未来可支持单框双向端口容量 12.8 Tbit/s。

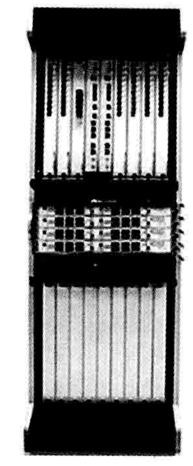


图 1-36 NE5000E 集群路由器

NE5000E 集群系统支持单框和多种集群模式，例如两框背靠背集群、一拖四集群、二拖八集群等，最多可达容量 200 TB 的 16 拖 64 集群系统。

2. 创新的 ISHE 技术

NE5000E 采用创新的 ISHE（In-Service Hardware Expansion，不间断硬件扩展）技术，可在业务不中断、硬件不更换的情况下，实现集群平滑扩容。未来，NE5000E 的端口容量可从 3.2 TB 平滑扩展到 200 TB，将具备最灵活的扩展性，满足运营商可持续发展的业务需求。NE5000E 采用创新正交矩阵设计架构实现光（电）交叉板和交换网板全连接，使数据流量最大程度地共享交换平面；集群高速连接光子卡支持弹性按需配置；交换芯片模式实现 Online 动态配置。这些亮点组合而成的 ISHE 方案提升了集群系统的可靠性，同时最大限度地保护了用户的原有硬件投资。

3. 领先的背靠背设计

NE5000E 可组合成独特的两框背靠背集群系统，省去中央交换框，为用户节省 OPEX（Operating Expense，运营成本）高达 40%。两框背靠背集群系统的端口容量双向可达 6.4 Tbit/s，可以满足未来 2～3 年业务发展需要，并且可平滑升级以支持更多框集群，是目前最佳的两框集群系统模式。

4. 首家端到端 100 Gbit/s

2009 年，华为业界首先发布端到端 100G NE5000E 集群系统，支持单端口 100 Gbit/s、10×10 Gbit/s 和 2×40 Gbit/s POS 等多种接口。通过 IP 和光的融合技术，华为提供了 100 GE+100 G WDM 全业务解决方案，支持客户按需灵活选择。NE5000E 采用华为自研 Solar 2.0 芯片，可持续满足未来海量带宽需求。100 Gbit/s 平台利用创新的非对称负载分担技术，实现了 100 Gbit/s 链路和原有 40 Gbit/s、10 Gbit/s 链路的非对称捆绑，最大限度地保护了客户原有 IP 和传输资源。LPUF-100 单板可以支持 1/4 槽位或 1/2 槽位多种灵活子卡，例如 5×10 GE 子卡、2×10 G POS 子卡和 40 G POS 子卡，可满足不同业务的应用需求。

5. 电信级可靠性

NE5000E 从多个层面进行了可靠性保证。首先是设备级别的保护。NE5000E 采用无源背板设计，所有关键组件支持热插拔与热备份，并且实现了基于状态的热切换和不间断的路由转发 NSF/NSR，同时提供热补丁技术及软件平滑升级。其次是基于网络级别的保护。NE5000E 提供 IGP 快速收敛、IP/LDP/TE 快速重路由、BGP/ISIS 自动快速重路由、BGP/ISIS/OSPF/LDP/PIM 协议辅助恢复、虚拟路由冗余协议 VRRP、BFD 链路快速检测、TRUNK 跨单板链路捆绑等保护机制，有效保证了全网运行的高速可靠。系统可靠性高达 99.999%。

6. 绿色集群

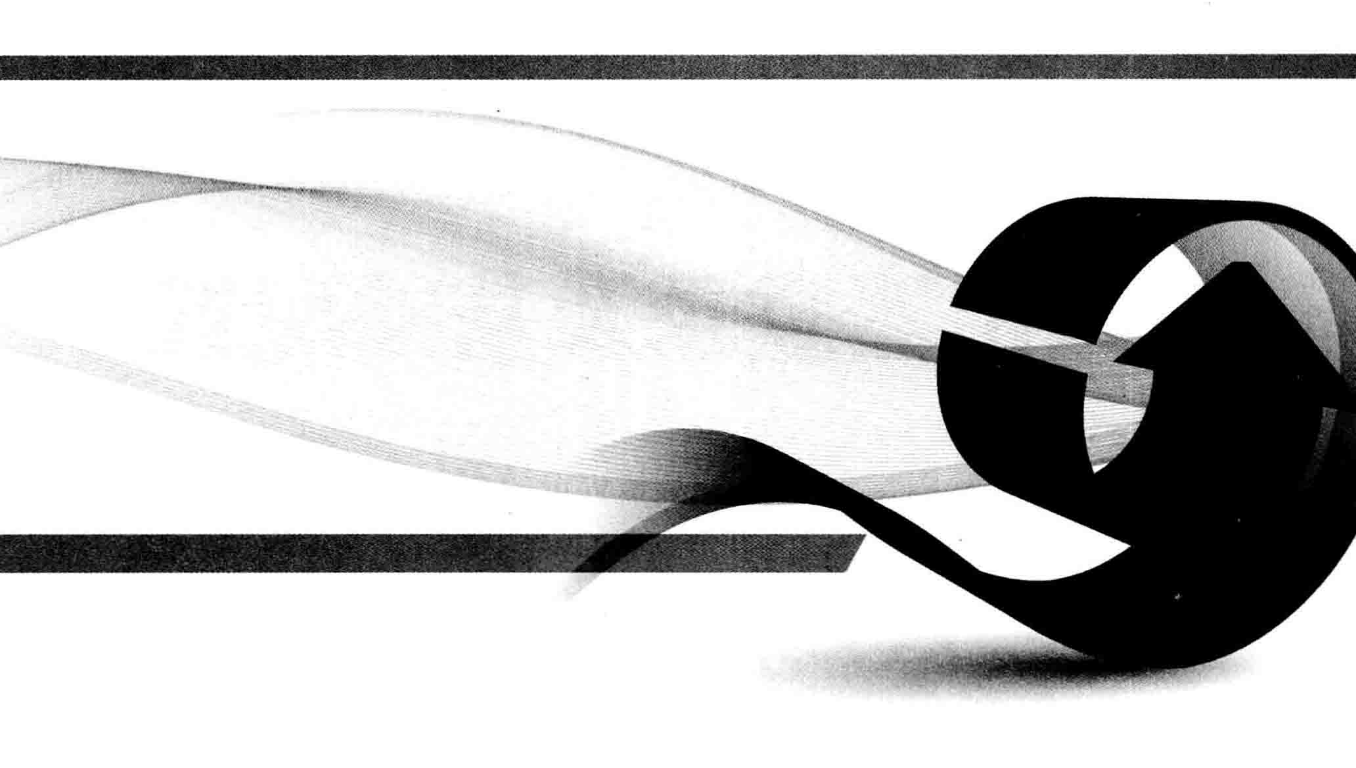
NE5000E 是一个真正的绿色集群路由器，绿色理念贯穿 NE5000E 的整个生命周期。NE5000E 关键芯片设计采用 65 nm 工艺，集成度提高，降低功耗 30%。在散热方面，采用专利技术的循环风散热技术，大大提高了散热效率，降低散热功耗 50%。NE5000E 采用新型材质和紧凑设计，体积小、重量轻，对地面承重无特殊要求，既可快速部署，又节省了机房改造工作量。NE5000E 集群真正实现了设计、部署、运行全“绿色”。

1.4.6 NE5000E 集群路由器的主要特性

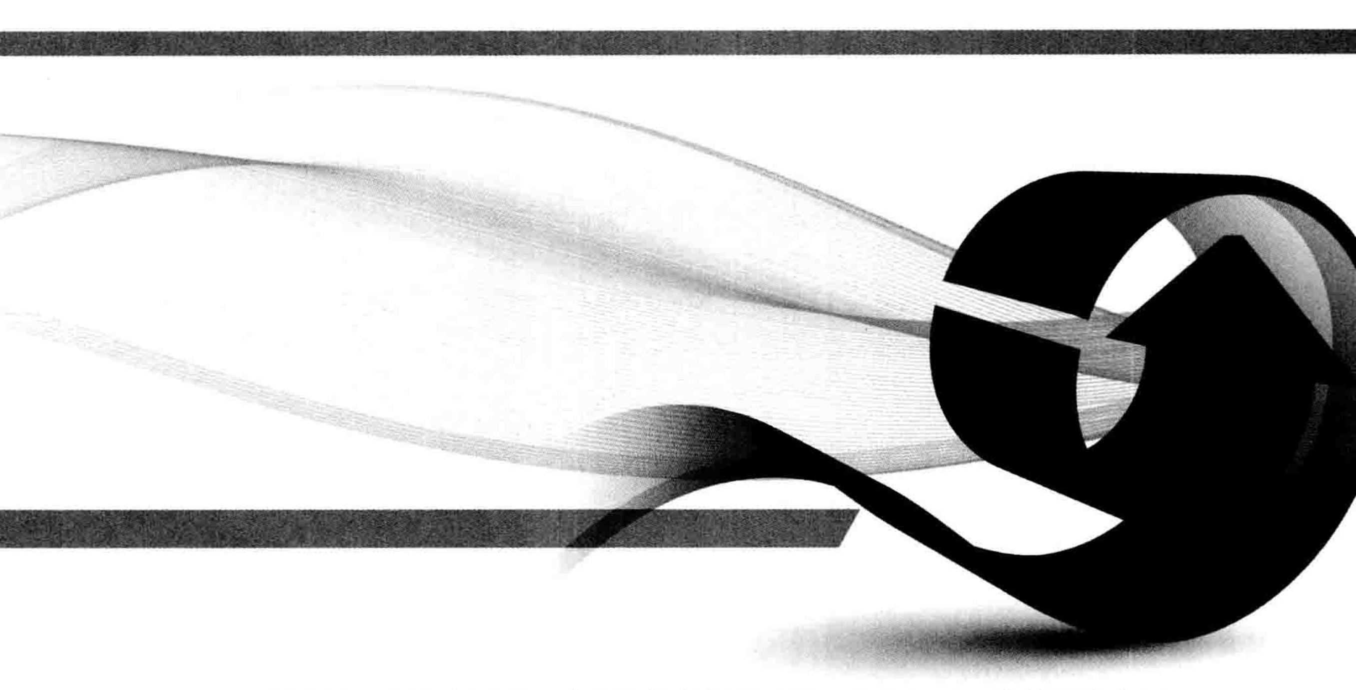
NE5000E 集群路由器的主要特性体现在集群性能和可靠性方面，具体如表 1-57 所示。

表 1-57 NE5000E 集群路由器主要特性

特性	NE5000E
吞吐容量	无阻塞交换结构，支持多机框集群。系统最大端口容量双向可达 200 Tbit/s/64 框
端口容量	3.2 Tbit/s/单机框（双向）
接口板槽位	16 槽位/单机框
接口类型	GE、10GE、OC768c POS、100 GE 等
路由协议	支持 IPv4 静态路由、OSPF、IS-IS、BGP-4、PIM，MSDP、MBGP 等路由协议
IPv6	• 全面支持 IPv4 和 IPv6 双协议栈。基于硬件方式实现 IPv6 线速转发处理 • 支持 IPv6 静态路由、OSPFv3、BGP4+、RIPng、IS-ISv6 等路由协议 • 支持 IPv6 邻居发现、PMTU 发现、TCP6、ping IPv6、Tracert IPv6、socket IPv6、TFTP IPv6、IPv6 策略路由和 IPv6 NetStream 等特性 • 提供 IPv6 PE、IPv6 over IPv4 等丰富的 IPv4 向 IPv6 的过渡技术
可靠性	• 主控模块 1:1 备份，交换网 3+1 备份，系统电源和风扇冗余备份 • 支持基于状态的热切换，不间断转发；支持不间断路由 • 支持 VRRP/BGP/OSPF/ISIS/TE LSP/LDP/LSP/TE/PIM BFD • 提供 IGP/BGP/组播快速路由收敛 • IP/LDP/BGP/TE 快速重路由（FRR）功能，BGP/ISIS 自动快速重路由，ETH 和 IP 链路捆绑 • 支持在线软件升级（ISSU）；智能错误诊断，热补丁



第2章 路由器登录及基础配置



新购买一台路由器后，首先要做的就是配置一些为以后正常使用路由器VRP系统配置和管理路由器而进行的基础配置，如主机名、时间和日期、管理IP地址、信息中心、Telnet登录所需的VTY用户界面、AAA验证配置，以及用于批量自动配置新设备所使用的U盘开局和Auto-Config功能等。

本章介绍的是AR G3路由器的各种登录方法（包括Console口/MiniUSB口本地登录、Telnet和Web远程登录）的配置，系统启动配置（包括系统软件、配置文件的更新、备份和下次启动指定等）和BootROM菜单功能及应用，以及信息中心、U盘开局和Auto-Config自动配置功能。这些都是我们在正式使用路由器VRP系统之前或者进行路由器系统安装和维护时所必须要掌握的。但要注意，为了避免本书与配套的《华为交换机学习指南》一书中的内容重复，有关VRP系统的基本使用和文件管理方法在本书中不做介绍，具体可以参见配套的《华为交换机学习指南》的第2章和第3章。

2.1 AR G3 系列路由器的登录

在 AR G3 系列路由器中支持的登录方式包括 Console 口本地登录，Telnet、SSH 远程登录，以及 Web 登录 4 种。

2.1.1 首次本地登录

当用户需要为第一次上电的设备进行配置时，可以通过 Console 口、MiniUSB 口或通过 Telnet 方式登录设备。

一块主控板提供一个 Console 口和一个 MiniUSB 口。将用户终端的串行端口与设备 Console 连接，可实现对设备的本地登录；或者将用户终端的 USB 口与设备 MiniUSB 口直接连接，可实现对设备的远程登录。

说明 在通过 MiniUSB 口登录设备前，需要在用户终端上安装 MiniUSB 口的驱动程序，**且 MiniUSB 口和 Console 口同时接入时，只有 MiniUSB 口可以使用。**

另外，AR150/150-S/160/200/200-S 系列的主控板不提供 MiniUSB 口，但提供多个 LAN 接口，用户终端的网卡可与任意一个 LAN 口连接，通过 Telnet 方式登录，实现对设备的远程配置。

因为有关通过 Console 口或者 MiniUSB 口进行首次本地登录华为 AR G3 系列路由器的方法与在《**华为交换机学习指南**》一书第 3 章 3.1 节介绍的华为 S 系列交换机的方法一样，故在此不再赘述，参见即可。

2.1.2 首次 Telnet 远程登录

当 AR150/150-S/160/200/200-S 系列路由器第一次上电需要进行配置和管理时，用户可以直接通过 Telnet 方式登录设备进行远程配置，只需要把担当 Telnet 客户端的用户终端与路由器 LAN 口连接即可。这几个系列的路由器在出厂时所有 LAN 口都属于 VLAN1，对应的 VLANIF1 接口的缺省 IP 为 192.168.1.1，并且在设备上已经使能了 Telnet 服务，缺省用户名为 admin，缺省密码为 Admin@huawei。用户就可以利用 VLANIF1 接口 IP 地址，以及所配置的缺省用户名和密码进行远程 Telnet 登录。具体步骤如下（用户终端 PC 以 Windows XP 系统为例）。

① 使用一条直通双绞线将 PC 机的网卡和路由器的任意一个 LAN 接口连接。但在此确保 PC 机的 IP 地址要与设备缺省的 VLANIF1 管理 IP 地址（192.168.1.1）在同一网段。

② 先后开启设备和 PC 机电源，PC 机启动后单击“开始>所有程序>附件>命令提示符”打开命令提示符。

③ 在命令提示符界面下输入 **telnet** 192.168.1.1 命令，按回车键后执行通过 Telnet 方式登录设备。

④ 按照以下提示输入缺省的用户名：admin，缺省的密码：Admin@huawei。按回车键后会出现<Huawei>用户视图提示，表示登录成功。

```
Username:admin
Password:
<Huawei>
```

说明 如果是其他AR G3系列路由器，则需要先通过Console口、MiniUSB口进行本地登录，设置通过Telnet服务进行远程登录的基本设置。**这方面也已在《华为交换机学习指南》第3章3.6.2小节有详细介绍**，不再赘述，参见即可。

如果要退出Telnet登录，可直接在Windows XP系统命令提示符界面中输入**quit**命令即可。

2.1.3　首次登录后的基本配置

通过以上三种方法首次登录后，首先要完成的就是路由器正常使用、Telnet远程登录、Web登录等所需的路由器设备基本配置，如配置设备的时间/日期（参见《华为交换机学习指南》第3章表3-1和表3-2）、设备名称/IP地址（见表2-1，IP地址用于除AR150/150-S/160/200/200-S系列之外的其他AR G3系列路由器的Telnet远程登录使用），以及Telnet用户的认证级别和方式（见表2-2）。

表2-1　设备名称和IP地址的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**sysname** *host-name* 例如：[Huawei] **sysname** RA	设置路由器名称，为1～246个字符，**支持空格，区分大小写** 缺省情况下，华为路由器的缺省主机名为"Huawei"
3	**interface** *interface-type interface-number* 例如：[RA] **interface** gigabitethernet 1/0/0	键入要配置IP地址的接口(可以是WAN口，或VLANIF1接口)，进入接口视图 【注意】如果通过WAN接口登录设备配置IP地址，请保证设备与PC间路由可达；如果通过VLANIF1接口登录设备配置IP地址，配置好后需使用新的IP地址重新登录
4	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[RA-GigabitEthernet1/0/0] **ip address** 129.102.0.1 255.255.255.0	为以上接口配置IP地址。命令中的参数和选项说明如下 • *ip-address*：指定接口的IP地址 • *mask*：二选一参数，指定所设置的IP地址对应的子网掩码 • *mask-length*：二选一参数，指定所设置的IP地址对应的子网掩码长度 缺省情况下，在接口上没有配置IP地址，可用 **undo ip address** *ip-address* { *mask* | *mask-length* } 命令删除接口的IP地址 【注意】**如果接口上已经有IP地址，则原IP地址被删除，**新配置的IP地址将被使用。对于AR150/150-S160/200/200-S系列，在出厂时所有LAN口均默认加入VLAN 1，并配置了VLANIF1的缺省IP地址为192.168.1.1/24，可以在任意LAN口将此IP地址作为管理IP地址使用，无需另外配置管理IP地址，当然仍可修改VLANIF1的IP地址

表 2-2 **Telnet 用户的级别和认证方式的配置步骤**

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**user-interface vty** *first-ui-number* [*last-ui-number*] 例如：[Huawei] **user-interface vty** 1 3	进入计划用于 Telnet 登录的 VTY 用户界面视图（有关 VTY 用户界面详细介绍参见《**华为交换机学习指南**》第 3 章 3.3 节）。命令中的参数说明如下 • *first-ui-number*：指定配置的第一个 VTY 用户界面相对编号，取值范围为 0～14 的整数 • *last-ui-number*：可选参数，指定配置的最后一个用户界面相对编号，同时进入多个用户界面视图。取值范围为 1～14 的整数，但要比 *first-ui-number* 参数值大 【说明】当网络管理员使用 Console 口、异步串口、Telnet 方式或者 SSH 方式登录设备的时候，系统会根据用户的登录方式分配一个当前空闲的、编号最小的某类型的用户界面用来管理、监控设备和用户间的当前会话。同一用户登录的方式不同，分配的用户界面也不同。每个用户界面有对应的用户界面视图，在用户界面视图下网络管理员可以配置一系列参数，比如用户登录时的认证方式、用户登录后的级别等，当用户使用该用户界面登录的时候，将受到这些参数的约束，从而达到统一管理各种用户会话连接的目的
3	**user privilege level** *level* 例如：[Huawei-ui-vty1-3] **user privilege level** 2	设置以上 VTY 用户界面的用户级别，取值范围为 0～15 的整数（值越大，级别越高） 缺省情况下，Console 口用户界面的用户级别是最高的 15 级，其他用户界面（包括 VTY 用户界面）的用户级别为最低级的 0 级，可用 **undo user privilege** 命令来恢复对应用户界面下的用户级别为缺省情况 【说明】为了限制不同用户对设备的访问权限，系统对用户进行了分级管理。用户的级别与命令级别对应，不同级别的用户登录后，只能使用等于或低于自己级别的命令，从而保证了设备的安全性。有关用户级别与命令级别的对应关系介绍参见《**华为交换机学习指南**》第 2 章 2.1.4 小节
4	**protocol inbound** { **all** | **telnet** } 例如：[Huawei-ui-vty1-3] **protocol inbound telnet**	（可选）配置 VTY 用户界面支持协议，但配置结果要待下次登录请求时才生效。命令中的选项说明如下。 • **all**：二选一选项，指定支持所有的协议，包括 SSH 和 Telnet • **telnet**：二选一选项，指定仅支持 Telnet 协议 缺省情况下，用户界面支持的协议是 Telnet，可用 **undo protocol inbound** 命令恢复为缺省配置
5	**acl** *acl-number* { **inbound** | **outbound** } 例如：[Huawei-ui-vty1-3] **acl** 3001 **inbound**	（可选）配置用户界面的基于 ACL 的登录限制。仅当需要限制某个 IP 地址或 IP 地址段的用户可以登录到设备，或者限制已经登录的用户再从本设备登录到其他设备时才需要配置本步骤。命令中的参数和选项说明如下

（续表）

步骤	命令	说明
5	**acl** *acl-number* { **inbound** | **outbound** } 例如：[Huawei-ui-vty1-3] **acl** 3001 **inbound**	● *acl-number*：指定用于限制用户使用某个用户界面登录设备的 ACL 列表号，使用 2 000～2 999 范围的基本 ACL 可基于用户 IP 地址（即基于源 IP 地址）进行登录限制；使用 3 000～3 999 范围的高级访问控制列表可同时基于源 IP 地址和目的 IP 地址进行登录限制 ● **inbound**：二选一选项，限制某个 IP 地址或 IP 地址段的用户登录到本设备 ● **outbound**：二选一选项，限制已经登录的用户再从本设备登录到其他设备 缺省情况下，不对通过用户界面的登录进行限制，可用 **undo acl** [**ipv6**] { **inbound** | **outbound** }命令取消对通过用户界面登录进行对应的限制
6	**authentication-mode** { **aaa** | **password** } 例如：[Huawei-ui-vty1-3] **authentication- mode aaa**	设置以上 VTY 用户界面下的 Telnet 用户验证方式。命令中的选项说明如下 ● **aaa**：二选一选项，设置以上 VTY 用户界面下的 Telnet 用户验证方式为 AAA 验证方式。当配置用户界面的 AAA 验证方式时，系统将清除此用户界面已配置的密码。需要保存好登录用户名和密码，登录到设备时需要首先输入登录用户名和密码才能登录。登录到设备的用户所能访问的命令级别**由本表第 10 步**配置的本地用户的优先级级别决定 ● **password**：二选一选项，设置以上 VTY 用户界面下的 Telnet 用户验证方式为密码验证。需要保存好登录密码，登录设备时需要首先输入登录密码才能登录。登录到设备的用户所能访问的命令级别**由本表第 3 步**配置的用户界面所对应的级别决定。配置为此种验证方式时，需要先通过 **set authentication password cipher** 命令交互式配置本地验证的密码。本命令采用交互方式输入的密码不会在终端屏幕上显示出来。用户输入的密码必须符合以下要求 ➢ 输入的密码为字符串形式，区分大小写，长度范围是 8～128。在交互方式下设置密码时，可用 CTRL_C 组合键取消操作 ➢ 输入的密码至少包含两种类型字符，包括大写字母、小写字母、数字及特殊字符。特殊字符包括 `~!@#$%^&*()-_=+|[{}];:'", <.>/?和空格。**如果用户界面的验证方式是密码验证，但却没有配置密码，此时将无法成功登录设备** 缺省情况下，VTY 类型用户界面没有配置验证方式，可用 **undo authentication-mode** 命令用来删除用户界面的验证方式 【说明】**登录用户界面必须配置验证方式，否则用户下次无法通过该用户界面成功登录设备。**即当用户不是首次登录时（包括采用 Console 口登录），必须采用以上两种验证方式之一，否则用户无法成功登录设备。当用户首次通过 Console 口登录设备时，终端会提示设置登录密码，登录设备后，用户可以使用此命令重新设置验证方式；当 Telnet 或 SSH 用户首次通过 VTY 用户界面登录设备时，必须要使用此命令为登录的用户界面配置验证方式，配置完成后，仍可以使用此命令改变用户界面的验证方式

（续表）

步骤	命令	说明
7	（可选）配置用户界面的其他属性	**具体配置请参见《华为交换机学习指南》第3章3.5.1节的VTY用户界面的最大个数和3.5.3节的VTY用户界面的终端属性配置。**但这些VTY用户界面属性在设备上都有缺省值，用户一般不需要另外配置。但是可以根据用户使用需求，选择配置相关属性
8	**quit** 例如：[Huawei-ui-vty1-3] **quit**	退出用户界面视图，返回系统视图
9	**aaa** 例如：[Huawei] **aaa**	进入AAA视图，进行AAA验证信息配置。**以下各步仅当Telent登录采用AAA验证方式时才需要配置**
10	**local-user** *user-name* **password** {{ **cipher** | **irreversible-cipher** } *password* | **privilege level** *level*}* 例如：[Huawei-aaa] **local-user** user1@vipdomain **password cipher** huawei@1234 **privilege level** 3	配置Telnet用户登录用于AAA验证的本地用户名、密码和本地用户优先级。命令中的参数和选项说明如下 ● *user-name*：指定用户名，1～64个字符，**不支持空格，区分大小写**。如果用户名中带域名分隔符，如@，格式“user@domain”，则认为@前面的部分是用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域为默认域 ● **cipher**：二选一选项，表示对用户口令采用可逆算法进行了加密，非法用户可以通过对应的解密算法解密密文后得到明文密码，安全性较低 ● **irreversible-cipher**：二选一选项，表示对用户口令采用不可逆算法进行了加密，使非法用户无法通过解密算法特殊处理后得到明文密码，为用户提供更好的安全保障 ● *password*：可多选参数，指定本地用户登录密码。如果是**cipher**类型口令，为6～32个明文形式字符（仅PPP用户的显示密码长度范围是6～32个字符；Telnet等其他类型用户的显示密码长度范围是6～16个字符），或者32或者56位密文形式字符。如果是**irreversible-cipher**类型口令，则为6～32个明文形式字符，或者56位密文形式字符。但均不支持空格，区分大小写。**用户输入的密码必须包括大写字母、小写字母、数字和特殊字符中至少两种，且不能与用户名或用户名的倒写相同。**如果没有配置用户的密码，设备会自动为该用户指定一个缺省的密码admin@huawei.com ● *level*：可多选参数，指定本地用户的优先级，取值范围是0～15的整数，取值越大，用户的优先级越高。如果没有配置对应用户的级别，则采用VTY视图下通过本表第3步的**user privilege**命令配置对应的用户级别 可用**undo local-user** *user-name*命令用来删除指定的本地用户 【说明】本地管理用户登录设备后，可以创建、修改或删除同级别或低级别的其他本地用户的属性（例如密码、级别、最大接入数和有效期等）

（续表）

步骤	命令	说明
11	**local-user** *user-name* **service-type telnet** 例如：[Huawei-aaa]**local-user** user1@ vipdomain **service-type telnet**	配置指定本地用户的接入类型为 Telnet。参数 *user-name* 为 Telnet 用户名，与上一步中的该参数说明一样 缺省情况下，本地用户可以使用所有的接入类型（包括 8021x 用户、IP Session 用户、FTP 用户、HTTP 用户、PPP 用户、SSH 用户、SSL VPN 用户、Telnet 用户、Console 口用户、Web 认证用户等，可用 **undo local-user** *user-name* **service-type** 命令用来将本地用户的接入类型恢复为缺省配置

说明　完成基本配置（包括后面将要介绍的 Web 登录配置）后，要保存配置，以防配置信息丢失。保存配置的方法是在用户视图下执行 **save** 命令。有关配置文件的详细说明和管理请分别参见《华为交换机学习指南》第 2 章 2.4.2 小节和 2.5 节。

2.1.4　AR G3 系列路由器首次登录基本配置示例

本示例将介绍通过 Console 口首次登录 AR G3 路由器后，如何设置系统时间、设备名称、管理 IP 地址以及 Telnet 远程登录的 0～4 号 VTY 用户界面的用户级别、认证方式等基本配置。具体配置如下。

① 设置系统的日期、时间和时区，假设当前时间为 2013 年 9 月 20 号 14 点 10 分。

```
<Huawei> clock timezone BJ add 08:00:00
<Huawei> clock datetime 14:10:0 2013-09-20
```

② 设置设备名称（RA）和管理 IP 地址（GE0/0/0 接口 IP 地址：10.10.10.1/24）。

```
<Huawei> system-view
[Huawei] sysname RA
[RA] interface gigabitethernet 0/0/0
[RA-GigabitEthernet0/0/0] ip address 10.10.10.1 24
[RA-GigabitEthernet0/0/0] quit
```

③ 设置 0～4 号 VTY 用户界面的用户级别为 3，Telnet 用户 huawei（密码为可逆的 Huawei@123）的用户级别为 15，采用 AAA 认证方式。

```
[RA] user-interface vty 0 4
[RA-ui-vty0-4] user privilege level 3
[RA-ui-vty0-4] authentication-mode aaa
[RA-ui-vty0-4] quit
[RA] aaa
[RA-aaa] local-user huawei password cipher Huawei@123
[RA-aaa] local-user huawei privilege level 15
[RA-aaa] local-user huawei service-type telnet
[RA-aaa] quit
```

完成以上配置后，Telnet 用户可以 Telnet 方式远程登录设备。以 Windows XP 系统为例，在 Windows XP 系统命令行提示符下执行 **telnet** 10.10.10.1 命令，按 Enter 键后，在登录窗口输入用户名和密码（分别为 huawei 和 Huawei@123），验证通过后，会出现路由器的用户视图命令行提示符<RA>，如下所示。

```
Username:huawei
Password:
<RA>
```

2.2 Web 登录

通过本书第 1 章的学习我们已经知道，AR G3 系列路由器都可以通过 Web 方式进行设备配置与管理。在 AR G3 路由器内置一个 Web 服务器，则与路由器相连的终端（如用户 PC）可以通过 Web 浏览器访问。但要实现这一目的，首先要配置设备启用 Web 网管的方式，这仍需在本章前面介绍的首次登录后进行配置，具体配置任务包括以下几种。

① 设置设备管理 IP 地址（**请参见本章 2.1.3 节的表 2-1**）。

②（可选）通过 FTP 方式上传新的 Web 网页文件（将在 2.2.1 小节介绍，但如果使用系统自带的 Web 网页文件，则不需进行本步）。

③（可选）加载新的 Web 网页文件（将在 2.2.2 小节介绍，但如果使用系统自带的 Web 网页文件，则也不需进行本步）。

④ 创建 Web 网管账户。

⑤（可选）配置 HTTPS 服务器。

说明

AR G3 系列路由器的 Web 系统支持多浏览器，如 Firefox 4.0 及以上版本或者 IE 7.0 及以上版本。在使用 IE 浏览器时，安全级别不能设置为“高”，否则 Web 界面将无法显示。在使用 Firefox 浏览器时，请务必在浏览器菜单栏中选择“选项 > 内容”，勾选“启用 JavaScript”，然后在浏览器菜单栏中选择“选项 > 隐私”，勾选“接受站点的 cookie”和“接受第三方 cookie”，否则 Web 界面将无法显示。以上选项位置以 Firefox 4.0 为例说明，下文同。

当设备的软件版本变化后，例如软件版本的升级或者回退操作，使用 Web 网管前，建议清除浏览器缓存，否则页面显示可能会出现异常。使用 IE 浏览器时，请在浏览器菜单栏中选择“工具 > Internet 选项 > 常规”，单击“删除”按钮，勾选“Internet 临时文件”和“Cookie”，单击“删除”按钮清除浏览器缓存。使用 Firefox 浏览器时，请在浏览器菜单栏中选择“选项 > 隐私”，单击“清空近期历史记录”按钮，然后勾选“Cookie”和“缓存”，单击“立即清除”按钮清除浏览器缓存。

Web 系统不支持浏览器自带的后退、前进、刷新等按钮，使用这些按钮可能会导致 Web 页面直接回退到登录界面。

2.2.1 上传 Web 网页文件

AR G3 系列路由器自带的 VRP 系统中已包含了用于支持 Web 网管的 Web 网页文件，但如果想向路由器上传其他的 Web 网页文件，则可通过 FTP 方式从保存 Web 网页文件的 PC 中获取（事先要把所要上传的 Web 网页文件保存在对应的 PC 上）。

要使用 FTP 服务向路由器上传文件，首先要在路由器上配置好 FTP 连接的相关配置，如 FTP 服务器功能的启用、FTP 用户账户、FTP 用户访问的授权目录等。具体配置步骤如表 2-3 所示。

配置好后，可在 PC 操作系统命令提示符下远程访问开启了 FTP 服务器功能的路由器。现以 Windows XP 系统为例进行介绍。

表 2-3　　FTP 连接相关设置的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**ftp server enable** 例如：[Huawei] **ftp server enable**	使能路由器的 FTP 服务器功能
3	**aaa** 例如：[Huawei] **aaa**	进入 AAA 视图
4	**local-user** *user-name* **password cipher** *password* 例如：[Huawei-aaa] **local-user winda password cipher** 123456	配置本地 FTP 用户名和密码，有关参数说明请参见本章 2.1.3 小节表 2-2 第 10 步。**用户输入的密码必须包括大写字母、小写字母、数字和特殊字符中至少两种，且不能与用户名或用户名的倒写相同** 缺省情况下，系统中没有本地用户，**也不支持 FTP 匿名访问**
5	**local-user** *user-name* **service-type ftp** 例如：[Huawei-aaa] **local-user winda service- type ftp**	配置本地用户的服务类型为 FTP。缺省情况下，本地用户可以使用所有的接入类型，可用 **undo local-user** *user-name* **service-type** 命令将指定的本地用户的接入类型恢复为支持所有接入类型
6	**local-user** *user-name* **ftp-directory** *directory* 例如：[Huawei-aaa] **local-user** winda **ftp-directory** flash:/	配置本地 FTP 用户授权许可访问的路由器的存储器目录（包括完整的目录路径），为 1～64 个字符，不支持空格，**区分大小写** 当有多个 FTP 用户且有相同的授权目录时，可以执行 **set default ftp-directory** *directory* 命令为 FTP 用户配置缺省工作目录。此时，不需要通过本命令为每个用户配置授权目录 缺省情况下，本地用户的 FTP 目录为空，可用 **undo local-user** *user-name* **ftp-directory** 命令将指定的本地用户的 FTP 目录删除

① 在安装了 Windows XP 的 PC 上选择“开始 > 程序 > 附件 > 命令提示符”进入命令行提示符；然后在命令提示符中进入 Web 网页文件所在的目录，如 D:\ftp。

② 执行 Windows 命令 **ftp** 10.101.10.1（假设路由器的管理 IP 地址为 10.10.10.1），通过 FTP 方式登录路由器。根据提示输入之前设置的用户名和口令，按 Enter 键，当出现 FTP 客户端视图的命令行提示符，如 ftp>，此时用户进入了 FTP 服务器的工作目录，如图 2-1 所示。

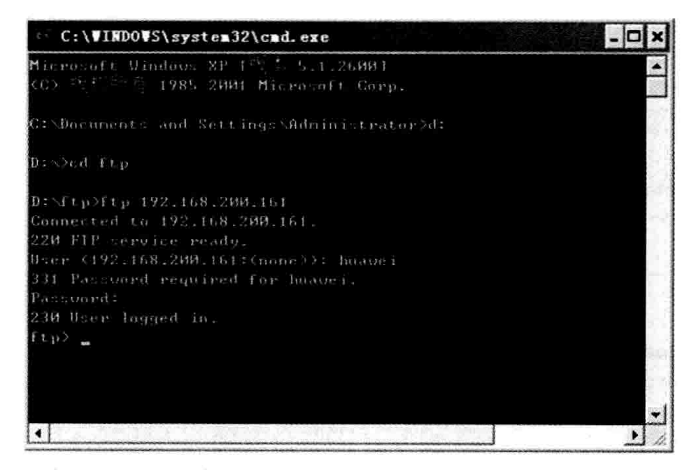


图 2-1　从 PC 端连接启用了 FTP 服务器功能的路由器界面

③ 在 PC 的 FTP 客户端视图的命令行提示符下执行 **binary** 命令，设置文件传输方式为二进制模式。

说明 FTP 支持 ASCII 码、二进制文件类型。二者的区别是：ASCII 传输使用 ASCII 字符，并由 Enter 键和换行符分开。二进制不用转换就可传输字符。

FTP 传输模式由客户端进行选择，系统默认 ASCII 方式。客户端可使用模式切换命令进行切换（ASCII 和 Binary）。传输文本文件使用 ASCII 方式，传输二进制文件使用 Binary 方式。此处为程序文件，故要使用 Binary 方式。

④ 执行命令 **put** web.zip 从 FTP 文件服务器端将 Web 网页文件上传到路由器，其中 web.zip 为 Web 网页文件名，如图 2-2 所示。

```
ftp> binary
200 Type set to I.
ftp> put web.zip
200 Port command okay.
150 Opening BINARY mode data connection for web.zip.
226 Transfer complete.
ftp: 发送 1339618 字节，用时 9.73Seconds 137.62Kbytes/sec.
ftp> _
```

图 2-2 向路由器上传 Web 网页文件的配置界面

⑤ 上传完成后，可在路由器的用户视图上（不是在 PC 的 FTP 客户端命令行视图中）执行 **dir** 命令查看当前存储目录下是否存在该系统文件。如果上传后发现路由器存储目录下的 Web 网页文件与源文件的大小不一致，则可能是在传输过程中出现异常，请重新传输。

2.2.2 加载 Web 网页文件

向路由器上传了 Web 网页文件后，还不能实现 Web 网管功能，还必须要在路由器上加载前面已上传的 Web 网页文件。Web 网页文件的格式为*.zip。但如果设备加载了新的软件大包，而软件大包中已包含 Web 网页文件，则可不必重新加载 Web 网页文件。

加载 Web 网页文件的步骤如表 2-4 所示。

表 2-4 加载 Web 网页文件的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**http server enable** 例如：[Huawei] **http server enable**	使能 HTTP 服务，但如果加载的 Web 网页不存在，HTTP 服务功能将无法使能 缺省情况下，HTTP 服务功能处于未使能状态，可用 **undo http server enable** 命令去使能 HTTP 服务功能
3	**http server load** *file-name* 例如：[Huawei] **http server load** web_1.zip	加载指定的 Web 网页文件。参数用来指定加载的 Web 网页文件名，必须是“*.zip”格式，5～64 个字符，不支持空格 缺省情况下，使能 HTTP 或者 HTTPS 服务功能后，设备默认加载系统软件包含的 Web 网页文件，可用 **undo http server load** 命令加载系统默认的网页文件

2.2.3　创建Web网管账号

与其他登录方式一样，采用Web登录方式，也需要配置专门的Web网管用户账户。Web网管的用户分为以下3个级别。

① 普通用户：对应用户级别1，业务用户使用，管理其增值业务。

② 企业管理员：对应用户级别2，企业的网络管理人员使用，管理企业内部局域网。

③ 超级管理员：对应用户级别3～15，运营商的网络管理人员使用，拥有最高权限。该级别用户可管理企业接入Internet网络，对设备管理维护。

用户级别为0或者未配置用户级别的用户不能登录Web网管。不同级别的Web用户对应的Web界面使用权限不一样，具体可参见产品手册说明（一般可直接使用最高权限进行配置）。

创建Web网管用户的配置步骤如表2-5所示。

表2-5　创建Web网管用户的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**aaa** 例如：[Huawei] **aaa**	进入AAA视图
3	**local-user** *user-name* **password** { { **cipher** |**irreversible-cipher** } *password*| **privilege level** *level*}* 例如：[Huawei-aaa] **local-user** winda **password cipher** huawei@123 **privilege level**	配置本地用户名、密码和用户级别，有关参数说明请参见本章2.1.3节表2-2第10步。**用户输入的密码必须包括大写字母、小写字母、数字和特殊字符中至少两种，且不能与用户名或用户名的倒写相同** 【注意】AR150/150-S/160/200/200-S系列缺省用户名为admin，密码为Admin@huawei，建议登录设备后及时更改密码（**但不能修改管理员账户**）并定时更新，以保证安全性
4	**local-user** *user-name* **service-type http** 例如：[Huawei-aaa] **local-user** winda **service- type http**	配置本地用户的服务类型为HTTP。缺省情况下，本地用户可以使用所有的接入类型，可用 **undo local-user** *user-name* **service-type** 命令将指定的本地用户的接入类型恢复为支持所有接入类型
5	**quit**	退出AAA视图，返回系统视图
6	**http timeout** *timeout* 例如：[Huawei] **http timeout** 5	（可选）配置HTTP会话的空闲等待时间，取值范围是1～35 791整数分钟。超时Web用户（目前最多支持同时5个Web用户）后将自动下线，HTTP服务器不会主动通知用户，而是等待用户发送下一次请求时再通知用户。而且，**本命令是覆盖式命令，以最后一次配置为准** 缺省情况下，会话超时时间为10 min，可用 **undo http timeout** 命令恢复HTTP服务器的超时时间到缺省值

2.2.4　配置HTTPS服务器

在某些恶劣的网络环境下（例如网络攻击较多，需要跨网络远程登录Web界面等），或者出于增强设备自身安全的考虑，可能会使用到通过HTTPS这种更为安全的协议来

登录 Web 界面。HTTPS 协议通过加密，可以保证管理员 PC 在通过 Web 界面管理设备的过程中，相关数据在网络中传输的安全性。

HTTPS 服务器的配置比较简单，具体配置步骤如表 2-6 所示。

表 2-6 HTTPS 服务器配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**ssl policy** *policy-name* **type server** 例如：[Huawei] **ssl policy** userserver **type server**	创建一个 SSL 策略并进入 SSL 策略视图，或者直接进入一个已创建的 SSL 策略视图。参数 *policy-name* 用来指定 SSL 策略的名称，为 1～31 个字符，只能包含下划线，字母和数字，**不区分大小写** 缺省情况下，路由器没有创建 SSL 策略，可用 **undo ssl policy** *policy-name* 命令用来删除一个指定的 SSL 策略
3	**pki-realm** *realm-name* 例如：[Huawei-ssl-policy-userserver] **pki- realm** deafault	配置 SSL 策略所使用的 PKI 域。参数 *realm-name* 用来指定 PKI 域的名称，1～15 个字符，不支持空格，不区分大小写，且不能包含字符“?” 缺省情况下，路由器没有配置 SSL 策略所使用的 PKI 域，可用 **undo pki-realm** 命令删除 SSL 策略所使用的 PKI 域 【说明】在服务器型 SSL 策略视图下，执行本命令配置 SSL 策略所使用的 PKI 域，SSL 服务器将基于 PKI 域从认证机构 CA 获取数字证书，以便 SSL 客户端根据数字证书对作为 SSL 服务器的 Router 进行身份验证，即当路由器作为 SSL 服务器时，允许 SSL 客户端对其进行身份验证，但它不具备对 SSL 客户端进行身份验证的功能。如果在同一个 SSL 策略视图下重复执行本命令时，则**新配置将覆盖老配置**
4	**quit** 例如：[Huawei-ssl-policy-userserver] **quit**	退出 SSL 策略视图，返回系统视图
5	**http secure-server ssl-policy** *ssl- policy* 例如：[Huawei] **http secure-server ssl-policy** userserver	配置 HTTPS 服务器关联的服务器型 SSL 策略。参数 *ssl-policy* 用来指定 HTTPS 服务器关联的服务器型 SSL 策略的名称 缺省情况下，未配置 HTTPS 服务器关联的服务器型 SSL 策略，可用 **undo http secure-server ssl-policy** 命令取消 HTTPS 服务器与服务器型 SSL 策略的关联 【注意】执行本命令配置 HTTPS 服务器关联的服务器型 SSL 策略后，作为 HTTPS 服务器的设备可以利用该 SSL 协议的数据加密、身份验证和消息完整性验证机制，保证用户和设备之间数据传输的安全性 在使用下一步的 **http secure-server enable** 命令使能设备的 HTTPS 服务器功能后，将不能够更改或删除 HTTPS 服务器关联的服务器型 SSL 策略。若需更改或删除关联的服务器型 SSL 策略，则应首先使用 **undo http secure-server enable** 命令去使能设备的 HTTPS 服务器功能

（续表）

步骤	命令	说明
6	**http secure-server enable** 例如：[Huawei] **http secure-server enable**	使能路由器的 HTTPS 服务器功能。执行本命令使能设备的 HTTPS 服务器功能后，设备将作为 HTTPS 服务器，利用 SSL 协议的数据加密、身份验证和消息完整性验证机制，保证用户和设备之间数据传输的安全性，这样用户即可以利用 Web 页面安全访问远程的设备。但在执行本步操作之前，需确保已使用上一步的 **http secure-server ssl-policy** 命令配置了 HTTPS 服务器关联的 SSL 策略，否则本命令不生效 缺省情况下，未使能设备的 HTTPS 服务器功能，可用 **undo http secure-server enable** 命令去使能设备的 HTTPS 服务器功能

在使能路由器的 HTTPS 服务器功能时会出现以下提示信息。最开始因为没有使能 HTTPS 服务器功能，所以会在提示信息中要求确认是否要使能 HTTPS 服务器功能，按 Y 键即可。

```
[Huawei] http secure-server enable
Warning: The HTTP server has not configured with SSL policy. Continue starting HTTP secure server? [Y/N]: y
  This operation will take several minutes, please wait......................................................
Info: Succeeded in starting the HTTPS server
[Huawei] quit
```

当用户在主机上打开浏览器，输入网址"**https:**//IP address"后，主机将以 HTTPS 的方式访问 Web 网管页面，用户后续可以利用 Web 网管页面安全访问和管理路由器。

2.2.5 登录 Web 网管

配置好以上各项配置任务后，接下来就可以正式进行 Web 网管登录了。在使用 Web 方式登录设备前，需完成以下任务。

① 设备的接入端口已配置 IP 地址。

说明　AR150/150-S/160/200/200-S 系列包含出厂缺省配置，其 IP 地址为 192.168.1.1、子网掩码为 255.255.255.0、接口为 VLANIF 1。如果未修改缺省配置，则 Ethernet0/0/0～Ethernet0/0/7 均可作为接入端口，接入端口的 IP 地址为 192.168.1.1。

② PC 终端和设备网络互通。

③ 路由器设备正常运行，HTTP 服务已正确配置。

④ PC 终端已安装浏览器软件。

Web 网管的运行环境如图 2-3 所示，用户可以使用 PC 通过 Web 网管对设备进行管理和配置。

下面是具体的登录步骤。

① 在 PC 终端上打开浏览器软件（以 IE7.0 为例），在地址栏中输入"http://192.168.1.1"（192.168.1.1 为示例，请以以太接口中实际配置的接入端口 IP 地址为准），按 Enter 键，显示 Web 网管的登录页面，如图 2-4 所示。

② 在 Web 管理界面中输入以下登录信息。

- 选择语言：目前支持中文和英文，默认根据浏览器的语言自动选择。

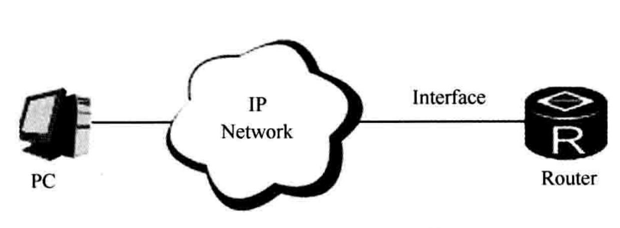


图 2-3 Web 网管使用环境

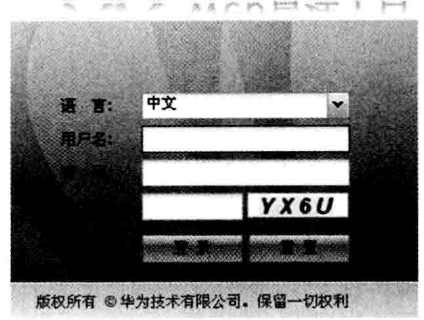


图 2-4 AR G3 路由器 Web 管理界面

• 用户名和密码：**admin** 为缺省的设备用户名，**Admin@huawei** 为缺省的设备登录密码。登录后可以在"系统管理 > 用户管理"页面创建或者修改用户。

• 验证码（字母不区分大小写）。如图片中的字符不易辨识，请单击"刷新"链接，获取新的验证码。

③ 以上信息正确输入后单击"登录"按钮，即可进入操作页面。如果需要重新输入所有登录信息，单击"重置"按钮，则清空输入的用户名、密码和验证码，且验证码自动刷新。

说明 登录时如果提示"登录用户已满"，表示当前通过 Web 方式登录的用户已达到上限（设备默认 Web 用户数目的上限为 5 个）。登录时如果提示"客户端 IP 地址无效"，表示当前登录主机的 IP 地址未在设备的信任列表中。登录时如果提示"输入密码出错次数已达上限 5 次，该用户被锁定。"，表示当前登录用户已经被锁定，账号在 15 min 后会自动解锁。

若要退出当前登录，可单击页面右上角的"注销"按钮，重新返回到如图 2-4 所示的登录页面。用户登录成功后，若在固定时间内未进行任何操作（缺省超时时间为 10 min），系统会自动注销当前登录。单击"确定"按钮后，重新返回到登录页面。

2.3 配置系统启动

设备启动时会启动保存在设备存储器中的系统软件和加载配置文件，用户可以管理这些设备系统软件和配置文件。AR150/150-S/160/200/200-S 系列、AR1200 系列、AR1200-S 系列、AR2201-48FE、AR2201-48FE-S、AR2202-48FE、AR2204-S、AR2204 和 AR2220L 支持的存储器为 Flash 或者 U 盘，AR2220、AR2220-S AR2240、AR2240-S 和 AR3200 系列支持的存储器为 Flash、Micro SD 卡或者 U 盘。**本章中涉及存储器的地方均以 Micro SD 卡为例。本节介绍的配置操作均在用户视图下进行。**

2.3.1　系统启动概述

系统启动时需要加载系统软件（包括 VRP 系统软件和 BootROM 软件）和配置文件。如果指定了下次启动的补丁文件，则还需加载补丁文件。

1. 进行系统启动的场景

需要进行系统启动的场景一般有以下几种。

（1）对设备进行升级操作，即系统软件从低版本至高版本升级

当增加了新特性或者需要对原有性能进行优化，以及解决当前运行版本落后的问题时，需要对设备进行升级。此时需要加载高版本的系统软件，并重新启动设备来完成加载。

（2）对设备进行降级操作（版本回退），即系统软件从高版本至低版本降级

设备完成升级后，如果业务出现异常，可以先将设备版本进行回退。此时需要加载低版本的系统软件，并重新启动设备来完成加载。

（3）在开局场景下，可以对一个新设备加载已有的满足用户需求的配置文件

新设备中只包含了设备出厂时的缺省配置，如果需要将这台新设备连接至网络再运行业务，则需要用户在设备上进行大量的配置，将会花费不少时间。对于这种情况，只须为这台新设备指定满足用户需求的配置文件，利用 U 盘开局功能重新启动设备即可进行自动配置，极大提升了用户对设备的配置效率。

（4）对设备指定升级后的补丁文件

可以在设备升级的同时指定之前未安装过的补丁文件，这样在设备升级完成后，补丁文件可同时生效。设备的升级与每次发布的版本相关，在发布新版本的同时会配套发布相应的升级指导书，用户可以根据升级指导书进行设备升级。升级指导书获取途径：请先登录华为公司企业业务支持网站（http://support.huawei.com/enterprise）；登录后，在“软件下载 > 产品软件 > 企业网络 > 路由器 > 接入路由器 > AR”路径下，根据产品型号和版本名称，获取相应的升级指导书。

2. 系统软件

设备的系统软件包括 VRP 系统软件和 BootROM 软件，扩展名为.CC。设备上电后，先运行 BootROM 软件，初始化硬件并显示设备的硬件参数，然后运行 VRP 系统软件。系统软件一方面提供对硬件的驱动和适配功能，另一方面实现了业务特性。BootROM 软件与系统软件是设备启动、运行的必备软件，为整个设备提供支撑、管理、业务等功能。

设备在升级时将同时升级 VRP 系统和 BootROM 软件。目前，设备的系统软件中已经包含了 BootROM 软件，在升级 VRP 系统软件的同时即可自动升级 BootROM。

3. 配置文件

配置文件是用户在配置设备时所输入的命令行集合。用户将当前配置保存到配置文件中，以便设备重启后，这些配置能够继续生效。另外，通过配置文件，用户可以非常方便地查阅配置信息，也可以将配置文件上传到别的设备，来实现设备的批量配置，如前面说的 U 盘开局配置和自动配置，具体将在本章后面介绍。

配置文件为文本文件，具有以下基本特性。

① 以命令格式保存。

② 为了节省空间，只保存非缺省的参数。

③ 以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以“#”开始的为注释行）。空行或注释行可以是一行或多行。

④ 文件中各节的顺序安排通常为：全局配置、接口配置、各种协议配置和用户界面配置。

⑤ 配置文件必须以“.cfg”或“.zip”作为扩展名，而且**必须存放在存储设备的根目录下。**

设备配置文件分为“出厂配置”、“配置文件”和“当前配置”这三种，区别如表 2-7 所示。

表 2-7　　出厂配置、配置文件和当前配置的区别

概念	描述	查看方式
出厂配置	设备在出厂时，通常会被安装一些基本的配置，称为出厂配置，用来保证设备在没有配置文件或者配置文件丢失、损坏的情况下，能够正常启动、运行。**但缺省情况下，AR150-S/200-S/AR1200/1200-S/2200/2200-S/3200 系列没有出厂配置**，必须在用户视图下执行命令 **set factory-configuration from** { current-configuration | *filename* }，指定当前配置或设备上已有的配置文件作为设备的出厂配置	使用 **display factory-configuration** 命令查看设备的出厂配置信息
配置文件	设备上电时，从默认存储路径中读取配置文件进行设备的初始化操作，因此该配置文件中的配置称为初始配置。如果默认存储路径中没有配置文件，则设备用缺省参数初始化配置。在以后的运行中，用户保存的配置即可形成新的配置文件 缺省情况下，AR150/150-S/160/200/200-S 系列使用设备的出厂配置进行初始化操作	使用 **display startup** 命令可以查看到设备本次以及下次启动的配置文件；使用 **display saved-configuration** 命令可以查看设备下次启动时的配置文件信息
当前配置	与初始配置相对应，设备运行过程中正在生效的配置称为当前配置	使用 **display current-configuration** 命令查看设备的当前配置信息

用户可以在 CLI 下修改设备的当前配置，但为了使当前配置能够作为设备下次启动时的起始配置，需要使用 **save** 命令保存当前配置到默认存储器中，形成配置文件。

注意 在使用不完整格式的命令（如缩写，简化命令）进行配置时，由于命令保存到配置文件中时使用的是完整格式，可能导致配置文件中存在长度超过系统可正确执行的命令长度（最大为 510 个字符），这时在系统重启时，这类命令将无法恢复。

4. 补丁文件

补丁是一种与设备系统软件兼容的软件，用于解决设备系统软件少量且急需解决的问题，与 Windows 操作系统中的补丁文件性质相似。在设备的运行过程中，有时需要对设备系统软件进行一些适应性和排错性的修改，如改正系统中存在的缺陷、优化某功能以适应业务需求等。

补丁通常以补丁文件的形式发布，一个补丁文件可能包含一个或多个补丁，不同的补丁具有不同的功能。当补丁文件被用户从存储器加载到内存补丁区中时，补丁文件中的补丁将被分配一个在此内存补丁区中唯一的单元序号，用于标志、管理和操作各补丁。

（1）补丁分类

根据补丁生效对业务运行的影响，补丁分成热补丁和冷补丁。

① 热补丁（Hot Patch，HP）：可以在不中断业务，不影响业务运行的同时安装并立即生效（不用重启）的补丁。

② 冷补丁（Cold Patch，CP）：安装后必须要重启设备的补丁，重启过程会影响业务的正常运行。

根据补丁间的依赖关系，又可把补丁分为增量型补丁和非增量型补丁。

① 增量型补丁：是指对在其前面的补丁有依赖性的补丁。一个新的补丁文件必须包含前一个补丁文件中的所有补丁信息，且用户可以在不卸载原补丁文件的情况下直接安装新的补丁文件。

② 非增量型补丁：只允许当前系统安装一个补丁文件，具有排他性。如果用户安装完补丁之后希望重新安装另一个补丁文件，则需要先卸载当前的补丁文件，再重新安装并运行新的补丁文件。

目前，AR G3 产品发布的补丁类型都为热补丁与增量型补丁。在后续的描述中如无特别说明都是指此类补丁。

（2）补丁状态

每个补丁都有自身的状态，只有在用户命令行的干预下才能发生切换。补丁状态的详细信息如表 2-8 所示。

表 2-8　　补丁状态

状态	说明	各状态之间的转换关系
空闲态（Idle）	此时，补丁文件存储在设备的存储器中，但文件中的补丁还没有被加载到内存补丁区中	当用户将补丁从存储器中加载到内存补丁区后，补丁的状态将被设置为运行
运行（Running）	当补丁被存储在内存补丁区中，且被永久运行时，补丁就处于运行状态。当单板被复位后，此单板上在复位前处于运行状态的补丁将保持运行状态	用户可以卸载处于运行状态的补丁，使补丁从内存补丁区中被删除

5．补丁安装

为设备安装补丁也是设备升级的一种方式。补丁安装方式有以下两种。

① 一般均采用不中断业务的方式，即在设备运行过程中直接加载运行补丁，这也是热补丁的优势。这种安装方式的详细过程请参见随补丁版本同时配套发布的补丁说明书，用户可以根据补丁说明书进行补丁安装。

② 另外一种方式就是本章后面将要介绍的指定系统下次启动的补丁文件。这种方式需要设备重启之后补丁才能生效，一般用于设备升级的同时安装补丁文件。

2.3.2　保存配置文件

用户可以进行保存配置文件、比较配置文件、备份配置文件、恢复配置文件、清除配置和设置出厂配置等操作。本节介绍保存配置文件的方法。

用户通过命令行可以修改设备的当前配置，而这些配置是暂时有效的，如果要使当前配置在系统下次重启时仍然有效，则在重启设备前，需要将当前配置保存到配置文件

中。可以通过以下两种方法保存配置文件：自动保存配置和手动保存配置。

1. 自动保存配置

有两种互斥的自动保存方法，具体方法如表 2-9 所示（**都是在用户视图下操作**）。在自动保存时，如果接口板不在位（也就是没有安装在设备中），相关的配置可能会丢失。

表 2-9 自动保存配置方法

步骤	命令	说明
方法一：设置自动保存开关		
1	**autosave interval** *value* 例如：<Huawei> **autosave interval on**	设置自动保存开关。参数 *value* 是系统自动保存开关，选择 **on** 或者 **off**。系统自动保存包括系统配置数据自动保存和变更配置数据自动保存。当取值为 **on** 时，两种自动保存特性均开启，但仍可以同时用 **save** 命令对系统配置数据进行手动保存。当取值为 **off** 时，两种自动保存特性均关闭，设备需采用 **save** 命令手动保存方式 缺省情况下，自动保存开关为 off，未使能自动保存功能。但本开关与下面方法 2 中的 autosave time 开关互斥，即两个开关不能同时打开
2	**autosave interval** { *time* | **configuration** *time* } 例如：<Huawei> **autosave interval** 120	配置系统按时间间隔定时保存配置，仅当上一步配置的自动保存开关为 **on** 时有效。命令中的参数说明如下 ● *time*：二选一参数，设置自动保存的时间间隔，取值范围为（10～10 080）的整数分钟，缺省值为 1 440 min。这样，无论配置是否发生了变化，当设置的定时保存配置时间间隔到达时，系统都会定时保存配置 ● **configuration** *time*：二选一参数，设置**在配置发生变更**时自动保存变更配置数据的时间间隔（**如果配置没有发生变化，则不会进行自动保存**），取值范围为（2～1 440）的整数分钟，缺省值为 30 min 缺省情况下，系统自动保存配置的时间间隔是 0，即不启动定时自动保存配置功能
方法 2：设置定点保存开关		
1	**autosave time** *value* 例如：<Huawei> **autosave time on**	设置配置数据的定点保存开关。参数 *value* 是系统定点保存开关，选择 **on** 或者 **off**。取值为 **on** 时，定点保存功能打开，系统按用户设置的定点时间自动保存；取值为 **off** 时，系统定点保存功能关闭，需要在配置变更后进行手动保存。但本开关与 **autosave interval** 开关互斥，即两个开关不能同时打开 缺省值情况下，配置数据的定点保存开关为 off
2	**autosave time** *time-value* 例如：<Huawei> **autosave time** 24:0:0	设置自动保存配置数据的定点时间，设置了自动保存的定点时间，系统就会在设置的时间点自动保存。参数的 *time-value* 取值范围为 00:00:00～23:59:59 缺省情况下，系统自动保存配置的定点时间是 00:00:00

2. 手动保存配置

执行命令 **save** [**all**] [*configuration-file*]可保存当前配置。将当前配置保存到指定文件时，文件必须以“.zip”或“.cfg”作为扩展名，且系统启动配置文件**必须存放在存储设备的根目录下**。

执行 **save all** 命令时将会保存当前所有的配置（包括不在位的板卡的配置）到系统当前存储路径中。在第一次保存配置文件时，如果不指定可选参数 *configuration-file*，则

设备将提示是否将文件名保存为“vrpcfg.zip”，配置信息将保存至系统当前启动配置文件里，执行 **display startup** 命令可以查看系统当前启动配置文件的文件名。

在用户视图下执行 **pwd** 命令，可以查看系统当前存储路径；在用户视图下执行 **cd** 命令，可以更改系统当前存储路径。

2.3.3 比较配置文件

用户可以通过比较当前配置和下次启动的配置文件，查看哪些配置项是不一致的，决定是否需要将当前配置设置为下次启动时加载的配置文件。但所比较的配置文件必须以“.cfg”或“.zip”作为扩展名。

系统在比较出不同之处时，将从两者有差异的地方开始显示字符，（默认显示 120 个字符），如果该不同之处到文件末尾不足 120 个字符，将显示到文件尾为止。在比较当前配置和下次启动的配置文件时，如果下次启动的配置文件为空，或者下次启动的配置文件虽然存在，但是内容为空，系统将提示读文件失败。

比较当前配置和指定配置文件的方法是执行 **compare configuration** [*configuration-file* [*current-line-number save-line-number*]] 命令，命令中的参数说明如下。

① *configuration-file*：可选参数，指定需要与当前配置进行比较的配置文件名，长度范围为 5~48 个字符，不支持空格。如果不指定此可选参数，系统将比较当前的配置与下次启动的配置文件内容是否一致。

② *current-line-number save-line-number*：可选参数，分别用来指定从当前配置，指定配置的该行号开始比较。如果不指定此可选参数，则表示从指定的配置文件的首行开始进行比较。用来指定在发现配置文件不同之处后，跳过该不同处各自从指定的行继续进行比较。

【示例】比较当前的配置与下次启动的配置文件内容是否一致。从输出信息可以看出，这两个配置文件第 14 行不一致，并且分别列出了两个配置文件中的对应配置。

```
<Huawei> compare configuration
 The current configuration is not the same as the next startup configuration file.
 ====== configuration line 14 ======
 undo http server enable
#
 drop illegal-mac alarm
#
 vlan batch 10 to 11
#
 dot1x enable
#
set transceiver-monitoring disable
 ====== Configuration file line 14 ======
 http server enable
#
 drop illegal-mac alarm
#
 vlan batch 10 to 11
#
 dot1x enable
#
set transceiver-monitoring disable
```

2.3.4 备份配置文件

为防止设备意外损坏，导致配置文件无法恢复，可以通过以下 4 种方法进行配置文件备份。

- 直接屏幕复制。
- 备份配置文件到存储器中。
- 通过 TFTP 备份配置文件。
- 通过 FTP 备份配置文件。

1. 直接屏幕复制

在命令行界面上，执行 **display current-configuration** 命令，并复制所有显示信息到 TXT 文本文件中，从而将配置文件备份到维护终端的硬盘中。

2. 备份配置文件到存储器中

这种方法主要便于用户在设备的存储器中及时备份当前配置文件。在设备启动之后，使用如下命令在设备的存储器中备份配置文件。

```
<Huawei> save config.cfg                    !---保存配置文件
<Huawei> copy config.cfg backup.cfg         !---备份配置文件
```

如果备份配置文件不是保存在设备的默认存储器中，需要指定绝对路径。

3. 通过 TFTP 备份配置文件

此时是把路由器作为 TFTP 客户端，在 PC 上启动 TFTP 服务器应用程序，设置好下载配置文件的传输路径、TFTP 服务器 IP 地址和端口号。

然后在用户视图下执行 **tftp put** 命令，备份指定的配置文件。

```
<Huawei> tftp 10.110.24.254 put sd1:/config.cfg backup.cfg
```

4. 通过 FTP 备份配置文件

此时路由器作为 FTP 服务器，用于保存备份配置文件的 PC 作为 FTP 客户端。具体的配置步骤如下。

① 使能 FTP 服务器功能，并在 AAA 视图下创建一个用于 FTP 文件传输的用户账户（假设用户名为 huawei，密码为 asdasd@15481erp），并指定授权此用户可以访问担当 FTP 服务器的路由器存储器的目录为“sd1:”。

```
<Huawei> system-view
[Huawei] ftp server enable                                  !---使能 FTP 服务器功能
Info: Succeeded in starting the FTP server.
[Huawei] aaa
[Huawei-aaa] local-user huawei password cipher asdasd@15481erp
[Huawei-aaa] local-user huawei ftp-directory sd1:
[Huawei-aaa] local-user huawei service-type ftp             !---设置 FTP 用户允许接入的服务类型为 FTP
[Huawei-aaa] local-user huawei privilege level 15           !---设置 FTP 用户具有最高的 15 级权限
```

② 在 PC 上通过 FTP 客户端 **ftp** 命令与担当 FTP 服务器的路由器设备建立 FTP 连接（假设设备的 IP 地址是 10.110.24.254）。建立连接时要输入前面配置的用于认证的 FTP 用户名和密码。

```
C:\Documents and Setting\Administrator> ftp 10.110.24.254
Connected to 10.110.24.254.
220 FTP service ready.
User (10.110.24.254:(none)): huawei
```

```
331 Password required for huawei.
Password:
230 User logged in.
```

③ FTP 用户验证通过后，FTP 客户端显示提示符“ftp>”，在“ftp>”提示下键入 **binary**（二进制传输模式），并通过 **lcd** 命令设置 FTP 客户端存放上载的备份配置文件的目录路径。

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

④ 下面就可以进行备份配置文件的上传了。

在 PC 上，使用 **get** 命令将配置文件下载至本地指定目录中，并保存为 backup.cfg。

```
ftp> get sd1:/config.cfg backup.cfg
```

确认 config.cfg 和 backup.cfg 的文件大小是否一致。如果文件大小一致则认为备份成功。

2.3.5 恢复配置文件

用户进行了错误的配置，导致功能异常，可以通过以下三种方法进行配置文件恢复。在配置文件恢复后，需要先使用 **startup saved-configuration** *configuration-file* 用户视图命令指定重新启动时使用的配置文件（如果新指定的配置文件没有变，则可不进行此步操作），然后使用 **reboot** 命令重新启动设备，使新的配置文件生效。

- 从存储器恢复配置文件。
- 通过 TFTP 恢复备份在 PC 上的配置文件。
- 通过 FTP 恢复备份在 PC 上的配置文件。

1. 从存储器恢复配置文件

这种方法主要便于用户将存储在设备存储器中的备份配置文件恢复成当前系统运行的配置文件。在设备正常工作时，使用如下命令。

```
<Huawei> copy sd1:/backup.cfg sd1:/config.cfg
```

2. 通过 TFTP 恢复备份在 PC 上的配置文件

此时路由器设备是作为 TFTP 客户端，具体的操作方法与 2.3.4 小节介绍的“通过 TFTP 备份配置文件”中的备份步骤相同，差别仅在于在命令行界面中执行携带 **get** 参数的 **tftp** 命令，将存储在 PC 上的配置文件 backup.cfg 下载到设备的 sd 中。具体命令如下。

```
<Huawei> tftp 10.110.24.254 get sd1:/backup.cfg config.cfg
```

3. 通过 FTP 恢复备份在 PC 上的配置文件

此时路由器设备作为 FTP 服务器，具体的操作步骤与 2.3.4 小节介绍的“通过 FTP 备份配置文件”中的备份步骤相同，差别仅在于第（4）步中在命令行界面中要执行 **put** 命令（前面 3 步是完全一样的），将存储在 PC 上的配置文件 backup.cfg 上传到设备的存储器中。第（4）步的具体命令如下。

```
ftp> put backup.cfg sd1:/config.cfg
```

2.3.6 清除配置

在以下情况下需要清除配置文件。

① 设备软件升级之后，原配置文件与当前软件不匹配。

② 配置文件遭到破坏，或加载了错误的配置文件。

清空配置的方法就是在用户视图下执行 **reset saved-configuration** 命令，清空设备下次启动使用的配置文件的内容，**并取消指定系统下次启动时使用的配置文件**（清空后需要使用 **startup saved-configuration** *configuration-file* 命令重新指定），从而使设备配置**恢复到出厂配置**。但清空后要使用 **reboot** 命令重启设备，使配置生效。

注意 执行该命令后，用户手动重启设备时，系统会提示用户是否保存配置，这时候选择不保存才能清空配置。**如果当前启动配置文件与所配置的下次启动配置文件相同，当前启动的配置文件也会被清空，一定要注意**。如果设备下次启动的配置文件为空，在执行本命令后，设备会提示配置文件不存在。如果不使用 **startup saved-configuration** *configuration-file* 命令重新指定含有正确配置信息的配置文件，或者保存配置文件，则设备下次启动时，将采用设备的出厂配置启动，若设备没有出厂配置，则采用缺省配置启动。

2.3.7 设置设备的出厂配置

用户可以根据需求把符合实际环境要求的基本配置设置为出厂配置，这样在执行了恢复出厂配置操作后就不需要再次配置这些基本信息了。具体的配置步骤如表 2-10 所示。

表 2-10 设置设备的出厂配置的配置步骤

步骤	命令	说明
1	**set factory-configuration from** { **current-configuration** | *filename* } 例如：<Huawei> **set factory-configuration from current-configuration**	指定当前配置或设备上已有的配置文件作为设备的出厂配置。命令中的参数和选项说明如下 ● **current-configuration**：二选一选项，将当前配置作为设备的出厂配置 ● *filename*：二选一参数，指定将作为设备的出厂配置的本地配置文件名，5～64 个字符，不区分大小写，扩展名必须为.cfg 和.zip 【说明】使用本命令指定了新的出厂配置后，AR150/150-S/160/200/200-S 系列通过长按设备上的 **reset** 按钮（5 s 以上），使设备的配置恢复至新的出厂配置。而 AR1200/1200-S/2200/2200-S/3200 系列则要通过执行本表第 3 步中的 **factory-configuration reset** 命令设置设备重启后恢复为新的出厂配置 另外，执行本命令后，新的出厂配置会覆盖原来的出厂配置，请慎用。在指定新的出厂配置时，新的配置文件大小不能大于 100 KB。如果大于 100 KB，在指定出厂配置时会失败，提示的如下错误信息：Error: Local file is too large!
2	**set factory-configuration operate-mode** { **reserve-configuration** | **delete-configuration** } 例如：<Huawei> **set factory-configuration operate-mode reserve-configuration**	（可选）指定恢复出厂配置时的操作方式为保留模式（选择 **reserve-configuration** 二选一选项时）或者删除模式（选择 **delete-configuration** 二选一选项时）。如果指定恢复出厂配置时的操作方式为保留模式，则在恢复出厂配置后，原来的配置文件会被保留。如果指定恢复出厂配置时的操作方式为删除模式，则在恢复出厂配置后，原来的配置文件不会被保留。缺省为保留模式

（续表）

步骤	命令	说明
3	**factory-configuration reset** 例如：<Huawei> **factory-configuration reset**	（可选）设置设备重启后恢复为出厂配置，**仅当下一次启动时需要恢复为出厂配置时才进行本步操作** 缺省情况下，设备重启后不会恢复出厂配置，如果用户没有设置配置文件为设备的出厂配置，执行此命令重启设备后，设备将采用缺省的配置参数进行初始化启动 【说明】AR150/150-S/160/200/200-S 系列还支持通过长按设备上的 **reset** 按钮（5 s 以上），使设备的配置恢复至出厂配置
4	**system-view** 例如：<Huawei> **system-view**	进入系统视图
5	**factory-configuration prohibit** 例如：[Huawei] **factory-configuration prohibit**	（可选）取消长按 **reset** 键恢复出厂配置的功能，设备重启后不恢复出厂设置。成功执行此命令，长按 reset 键，设备重启后不恢复出厂设置。**仅 AR150/150-S/160/200/200-S 系列支持此命令** 缺省情况下，长按 **reset** 键，设备重启后恢复出厂设置，可用 **undo factory-configuration prohibit** 命令设置长按 **reset** 键恢复出厂配置的功能
6	最后，可以在任意视图下执行 **display factory-configuration** 命令查看设备的出厂配置信息；执行 **display factory-configuration operate-mode** 命令查看设备恢复出厂配置时的操作方式（保留模式 Reserved 或者删除模式 Delete）	

2.3.8　配置系统启动文件

配置系统启动文件包括指定系统启动时使用的系统软件和配置文件，这样可以保证设备在下一次启动时以指定的系统软件启动，并以指定的配置文件初始化配置。如果系统启动时还需要加载新的补丁，则还需指定补丁文件。

在进行配置前，用户可以使用 **display startup** 命令查看当前设备本次及下次启动相关的系统软件、备份系统软件、配置文件、License 文件、补丁文件以及语音文件，如下所示。

```
<Huawei> display startup
MainBoard:
  Startup system software:                sd1:/basicsoftware.cc   !---显示本次启动所使用的系统软件文件
  Next startup system software:              sd1:/basicsoftware.cc   !--- 显示用户通过 startup system-software system-file 命令配置的下次启动时所使用的系统软件。如果没有配置则显示为本次启动时所使用的系统软件
  Backup system software for next startup:   null   !---显示下次启动时的备份系统软件，没有配置则为 null
  Startup saved-configuration file:          sd1:/vrpcfg.zip   !---显示本次启动时所用的备份软件
  Next startup saved-configuration file:       sd1:/vrpcfg.zip   !--- 显示用户通过 startup saved-configuration configuration-file 命令配置的下次启动时所使用的配置文件。如果没有配置则显示为本次启动时所使用的配置文件
  Startup license file:        null   !--- 显示系统本次启动时所使用的 License 文件，没有配置则为 null
  Next startup license file:     null   !---显示系统重新启动时所使用的 License 文件，没有配置则为 null
  Startup patch package:        null   !---显示系统本次启动时所使用的补丁包文件，没有配置则为 null
  Next startup patch package:     null   !--- 显示用户通过 startup patch file-name 命令配置的下次启动时所使用的补丁文件，没有配置则为 null
  Startup voice-files:         null   !---显示本次启动所使用的语音文件，没有配置则为 null
  Next startup voice-files:       null   !--- 下一次启动所使用的语音文件，没有配置则为 null
```

在配置系统启动文件时，需要注意以下几个方面。

① 如果没有配置设备下次启动时加载的系统软件，则下次启动时将默认启动此次

加载的系统软件。当需要更改下次启动的系统文件（如设备升级）时，则需要指定下次启动时加载的系统软件，此时还需要提前将系统软件通过文件传输方式保存至设备。**系统软件必须存放在存储器的根目录下，文件必须以“.cc”作为扩展名。**

② 如果没有配置下次启动时加载的配置文件，则下次启动将采用缺省配置文件（如vrpcfg.zip）。如果默认存储器中没有配置文件，则设备启动时将使用缺省参数初始化。**配置文件必须存放在存储器的根目录下，文件必须以“.cfg”或“.zip”作为扩展名。**

③ 补丁文件的扩展名为“.pat”，**也需要保存至设备存储器的根目录下。**

系统启动文件的配置步骤如表 2-11 所示。

表 2-11　　设置设备的出厂配置的配置步骤

步骤	命令	说明
1	**startup system-software** *filename* [**verify**] 例如：<Huawei> **startup system-software** basicsoft.cc	指定设备下次启动时加载的系统软件。命令中的参数和选项说明如下 ● *filename*：指定下次启动时加载的系统软件的文件名，1～64 个字符（文件名取值不带全路径时最大长度为 57 个字符），格式为[*drive-name*] [*path*] [*file-name*]，不支持空格，不区分大小写。如果未指定 *drive-name*，则此值为默认的存储器名 ● **verify**：可选项，指定对系统软件进行合法性检查，如果检查不通过，则配置不生效。避免了因为加载不合法的系统软件导致系统下次无法正常启动的问题
2	**startup system-software** *filename* **backup** 例如：<Huawei>startup **system-software** sd1:/basicsoft.cc **backup**	（可选）设置系统启动时所用的备份系统软件文件名，参数 *filename* 的说明同上一步的该参数说明。备份系统软件的主要作用是当启动时指定的系统软件出现损坏时，则系统可以调用备份的系统文件进行启动。备份系统软件可以和当前启动的系统软件完全相同，也可以是不同版本的系统软件文件，但前提是该系统软件一定能保证系统正常启动 缺省情况下，AR150/150-S/160/200/200-S 系列、AR1200/1200-S 系列、AR2201-48FE、AR2202- 48FE、AR2204 和 AR2220L 没有备份系统软件，AR2220/2200-S、AR2240、AR3200 系列的备份系统软件为 **sys_backup.cc**
3	**startup saved-configuration** *configuration-file* 例如：<Huawei> **startup saved-configuration** vrpcfg.cfg	指定系统下次启动时使用的配置文件。参数 *configuration-file* 用来指定下次启动时要使用配置文件的文件名，但此文件必须存在，且必须存放在存储设备的根目录下，为 1～64 个字符，**不支持空格，不区分大小写** 配置文件必须以*.zip 或者*.cfg 作为扩展名，其中，*.cfg 为纯文本格式，可直接查看其内容。指定为配置文件后，启动时系统对里面的命令逐条进行恢复。*.zip 是*.cfg 的压缩，占用空间较小。指定为配置文件后，启动时先解压成*.cfg 格式，然后逐条恢复 设备上电时，默认从存储器根目录中读取配置文件进行初始化
4	**startup patch** *file-name* 例如：<Huawei> **startup patch patch.pat**	（可选）指定设备下次启动时加载的补丁文件。参数 *file-name* 用来指定下次启动时所加载的补丁文件名，为 1～64 个字符（文件名取值不带全路径时最大长度 57 个字符），不区分大小写，不支持空格，格式为[*drive-name*] [*path*] [*file-name*]。如果未指定 *drive-name*，则此值为默认的存储器名

（续表）

步骤	命令	说明
4	**startup patch** *file-name* 例如：<Huawei> **startup patch patch.pat**	【注意】本命令是可覆盖型命令，如果用户再次使用本命令重新指定下次启用的补丁，则上一次的信息将被覆盖。执行完本命令，当设备重新启动后，系统将加载补丁并运行补丁。如果用户希望系统重新启动后不自动启用该补丁文件，则可以使用 **patch delete all** 命令删除当前补丁
5	配置完系统启动文件后，可使用 **display startup** 命令查看系统下次启动相关的系统软件、配置文件以及补丁文件	

2.3.9　重新启动设备

为了使上面各节配置加载的系统软件及相关文件生效，需要在配置完系统启动文件后，对设备进行重新启动。

重新启动设备有以下两种方式。

① 立即重新启动设备：执行命令行后立即重新启动。

② 定时重新启动设备：可设置在未来的某一时刻重新启动设备。

设备重启后，先以设置的下次启动软件包进行重启，如果用于下次启动的软件包被破坏，则以系统备份软件包启动，如果仍然失败，设备将在存储器上搜索合法的软件包启动（搜索顺序：flash→SD 卡→U 盘），如果某一存储器存在多个合法的软件包，则选用找到的第一个进行启动，否则系统将会反复执行整个操作流程。

说明　设备每一次重新启动的相关信息都会被详细记录下来，包括重新启动的次数、详细信息以及原因等，可以通过 **display reset-reason** 命令进行查看。

一般情况下，不要轻易重新启动设备，因为这将导致网络在短时间内瘫痪。在重新启动设备之前，如果需要使当前配置在重新启动设备后仍生效，应先确保当前配置已保存。

1. 立即重启动设备

要立即重启路由器设备，可在用户视图下执行 **reboot [fast]** 命令实现对设备的重新启动。如果选择了 **fast** 可选项，则表示快速重启设备，不会提示是否保存配置文件，否则会提示用户保存配置文件。

2. 定时重启动设备

要定时重启路由器设备，可先在用户视图下执行 **schedule reboot** { **at** *time* | **delay** *interval* }命令使能定时重新启动功能。命令中的参数说明如下。

① **at** *time*：二选一参数，设置设备定时重新启动的具体时间，格式为 *hh:mm YYYY-MM-DD*（其中 *YYYY-MM-DD* 为可选参数，如果指定的时间是在当天，则可不用输入），必须大于设备的当前时间，且与当前时间的差值范围小于 720 小时。如<Huawei> **schedule reboot at** 22:00（设置设备在当天晚上 22:00 重新启动）。

② **delay** *interval*：二选一参数，设置设备在定时重新启动前等待的时间，格式为 *hh:mm* 或 *mm*，等待的时间最大不超过 720 小时，*hh:mm* 中的 *hh* 表示小时，取值范围是

0～720 的整数，其中的 *mm* 表示分钟，取值范围是 0～59 的整数；*mm* 表示分钟，取值范围是 0～43 200 的整数。如<Huawei> **schedule reboot delay** 2:10（设置设备在 2 个小时 10 分钟后重新启动）。

如果配置了定时重启功能，可以执行 **display schedule reboot** 命令查看设备以上定时重启的相关配置。

2.3.10 系统启动配置示例

假设设备当前的系统软件版本已经不能满足用户需求，用户需要部署更多的特性。此时需要远程为该设备进行系统软件升级。

1. 基本配置思路分析

本示例的基本配置思路如下（先通过 Console 口登录设备）。

① 将新的系统软件上传至设备根目录。

② 保存系统当前配置，以使升级后配置仍生效。

③ 配置设备下次启动时加载的系统软件和配置文件。

④ 重新启动设备实现设备的升级。

2. 具体配置步骤

本示例的具体配置步骤如下。

① 将新的系统软件上传至设备根目录。

在进行配置前，可以先执行 **display startup** 命令查看当前设备的下次启动文件的配置情况，如有必要，可记下当前、下次启动时所用的系统软件/配置文件名称，如输出信息中的粗体字部分。

```
<Huawei> display startup
MainBoard:
  Startup system software:                  sd1:/basicsoft.cc
  Next startup system software:             sd1:/basicsoft.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:         sd1:/vrpcfg.zip
  Next startup saved-configuration file:    sd1:/vrpcfg.zip
  Startup license file:                     null
  Next startup license file:                null
  Startup patch package:                    null
  Next startup patch package:               null
  Startup voice-files:                      null
  Next startup voice-files:                 null
```

采用文件传输方式将新的系统软件文件上传至设备。文件传输方式较多（**具体可参见《华为交换机学习指南》第 3 章 3.7 节**），此处仅以 FTP 传输方式为例进行介绍。将路由器设备配置为 FTP 服务器，从 PC 客户端获取系统软件文件。上传文件前需确保路由器存储器有足够的空间保存新的系统软件文件，若空间不足，需要清理存储器。具体配置步骤如下（**可参见本章 2.2.1 小节**）。

```
<Huawei> system-view
[Huawei] ftp server enable
[Huawei] aaa
[Huawei-aaa] local-user huawei password cipher Huawei@123
[Huawei-aaa] local-user huawei service-type ftp
```

```
[Huawei-aaa] local-user huawei ftp-directory sd1:
[Huawei-aaa] local-user huawei privilege level 15
[Huawei-aaa] quit
[Huawei] quit
```

配置好 FTP 服务器功能后，在用户终端 PC 的命令行提示符下执行 **ftp** 10.1.1.1（假设路由器管理 IP 地址为 10.1.1.1，**管理 IP 地址的配置方法参见 2.1.3 小节表 2-3**）命令并成功与设备建立 FTP 连接后，使用 **put** 命令向设备上传新的系统软件文件 newbasicsoft.cc，包括的命令如下。

```
ftp>ftp 10.1.1.1
ftp>binary      !---设置为二进制传输模式
ftp>put newbasicsoft.cc
```

上传成功后，可执行 **dir** 命令查看上传后的系统软件文件，具体如下。输出信息中的粗体字部分就是新上传的系统软件。

```
<Huawei> dir
Directory of sd1:/

  Idx  Attr    Size(Byte)  Date            Time        FileName
    0  drw-             -  Apr 16 2012 13:19:58   logfile
    1  -rw-    85,925,409  Apr 16 2012 13:18:02   basicsoft.cc
    2  -rw-             4  Oct 27 2011 17:25:22   snmpnotilog.txt
    3  -rw-         6,033  Jul 16 2012 16:40:02   private-data.txt
    4  -rw-         3,275  Jul 14 2012 14:18:08   vrpcfg.zip
    5  drw-             -  Nov 14 2011 19:14:26   sysdrv
    6  drw-    88,239,759  Jul 16 2012 19:14:26   newbasicsoft.cc
...

1,927,220 KB total (1,130,464 KB free)
```

② 在路由器 CLI 用户视图下执行 **save** 命令保存系统当前配置。

```
<Huawei> save
```

系统将提示当前配置将保存至设备，是否继续，按 **y** 键后，系统提示当前配置已成功保存在设备中。

③ 配置设备下次启动时加载的系统软件和配置文件。

```
<Huawei> startup system-software newbasicsoft.cc
<Huawei> startup saved-configuration vrpcfg.zip
```

说明　在第②步配置完成后，可通过 **display startup** 命令查看下次启动文件的配置情况，可以看到"Next startup saved-configuration file:sd1:/**vrpcfg.zip**"，说明当前设备已经指定 **vrpcfg.zip** 作为下次启动时加载的配置文件，所以第③步配置下次启动时加载的配置文件步骤可以省略。但如果需要指定其他的配置文件作为下次启动时加载的配置文件，则必须要执行此步骤。

配置完成之后，执行 **display startup** 命令可查看设备下次启动时加载的系统软件和配置文件，如输出信息中的粗体字部分。

```
<Huawei> display startup
MainBoard:
  Startup system software:                    sd1:/basicsoft.cc
  Next startup system software:               sd1:/newbasicsoft.cc
  Backup system software for next startup:    null
  Startup saved-configuration file:           sd1:/vrpcfg.zip
```

```
Next startup saved-configuration file:        sd1:/vrpcfg.zip
Startup license file:                          null
Next startup license file:                     null
Startup patch package:                         null
Next startup patch package:                    null
Startup voice-files:                           null
Next startup voice-files:                      null
```

④ 重新启动设备。由于已在第②步保存过配置文件，且所设置的下次启动加载的配置文件仍为原来保存的配置文件，所以此时可以执行 **reboot fast** 命令进行快速重新启动。

```
<Huawei> reboot fast
```

系统会提示即将重新启动，是否继续，按 y 键即可。等候几分钟，设备重启完成后可再次进入系统。此时执行 **display version** 命令可看到设备当前的系统软件版本为新的版本。

2.4 BootROM 菜单

BootROM（Boot Read-Only Memory，启动只读内存）系统相当于 PC 中的 BIOS 系统，是路由器启动时首先要调用的软件系统，提供了配置恢复、系统软件升级等功能，是设备安全、维护的基础。

2.4.1 BootROM 简介

BootROM 是一组固化到交换机/路由器等设备主板上 ROM 芯片中的程序，保存着设备最重要的基本输入/输出的程序、系统设置信息、开机后自检程序和系统自启动程序。

当遇到以下情况时，可以通过 BootROM 菜单进行处理。

① 在系统崩溃，无法进入命令行操作界面时，可以通过 BootROM 菜单来恢复或者升级系统。这是 BootROM 系统菜单最重要的用途之一。

② 为防止丢失配置，可以通过 BootROM 菜单进行配置文件备份。

③ 为防止非法用户进入 BootROM 菜单，可以通过 BootROM 菜单来修改进入 BootROM 菜单的密码。

④ 当用户的 Console 口登录密码遗忘导致登录不进设备时，可以通过 BootROM 菜单配置跳过 Console 口用户登录密码，然后进行密码修改。

2.4.2 BootROM 主菜单

通过 Console 口连接设备，在设备重启过程中出现以下提示信息时，3 s 内（可通过 BootROM 菜单来修改等待时间，具体将在本节后面介绍）按 Ctrl+B 组合键，即可进入设备的 BootROM 系统。

```
Press Ctrl+B to break auto startup ... 3
```

按 Ctrl+B 组合键后会显示如下要求输入密码的提示信息，缺省情况下进入 BootROM 菜单的密码为 **huawei**，你可以通过 BootROM 菜单来修改缺省密码（具体将在本节后面介绍）。如果连续三次输入不正确的密码，系统将重新启动。这主要是为了保护 BootROM 系统不被非法进入、使用，以防乱修改。这与 PC 中 BIOS 系统也可设置进入密码一样。

```
Enter Password:******
```

进入BootROM系统后，首先显示的是如下BootROM系统主菜单（Main Menu），各菜单项的具体说明如表2-12所示。

```
            Main Menu

        1. Default Startup
        2. Serial Menu
        3. Network Menu
        4. Startup Select
        5. File Manager
        6. Reboot
        7. Password Manager

Enter your choice(1-7):
```

表2-12 BootROM主菜单中的子菜单说明

子菜单项	说明
1. Default Startup	默认启动子菜单。当BootROM系统修改的参数不会对BootROM菜单前面的初始化工作有影响时，可以使用此菜单项快速启动设备，避免重复初始化设备。**当用户需要快速启动设备时，可以执行此操作**。执行此操作，不会进入重启BootROM阶段，直接从当前阶段继续启动
2. Serial Menu	串口子菜单。当用户需要通过串口更新BootROM和CPLD（Complex Programmable Logic Device，复杂可编程逻辑器件）程序时，可以进入串口子菜单进行操作。但这项操作比较危险（可能导致芯片损坏），一定要慎重 通过串口更新BootROM和CPLD的优点是无需配置，直接连线后使用；缺点是文件传输速率慢
3. Network Menu	网络子菜单。当用户需要通过管理网口进行文件传输时，可以进入该子菜单进行操作 通过管理网口进行文件传输的优点是文件传输速率快，缺点是需要配置网络参数和文件服务器，并要保证设备和服务器路由可达
4. Startup Select	启动选项子菜单。当用户需要查看和修改启动配置信息时，可以进入该子菜单进行操作
5. File Manager	文件管理子菜单。当用户需要对文件系统进行管理和维护，可以进入该子菜单进行操作
6. Reboot	重启子菜单。当修改的参数对BootROM菜单前面的初始化工作有影响时，需要执行该子菜单先进入重启BootROM阶段，再继续启动
7. Password Manager	密码管理子菜单。为了防止非法用户进入BootROM菜单，可以进入此菜单修改进入BootROM菜单的密码。当用户的Console口登录密码遗忘导致无法登录设备时，也可进入此菜单配置跳过串口用户登录密码

2.4.3 串口子菜单

进入上节介绍的BootROM主菜单，选择第2项“2. Serial Menu”后即进入如下所示的“串口”子菜单。该子菜单中的4个菜单项说明如表2-13所示。

```
            Serial Menu

        1. Update Bootrom
        2. Update CPLD Chip 0
        3. Modify baud rate
        0. Return
```

```
Enter your choice(0-3):
```

表 2-13 串口子菜单的菜单项说明

菜单项	说明
1. Update Bootrom	通过串口更新 BootROM 软件
2. Update CPLD Chip 0	通过串口更新 CPLD 软件
3. Modify baud rate	修改串口参数。缺省情况下，传输速率为 9 600 bit/s。串口支持的传输速率有 9 600 bit/s、19 200 bit/s、38 400 bit/s、57 600 bit/s、115 200 bit/s。但如果修改串口传输速率，需要在 PC 端修改串口传输速率的设置与这里所设置的串口传输速率一致后要重新连接
0. Return	返回主菜单

2.4.4 网络子菜单

进入 2.4.2 小节介绍的 BootROM 主菜单，选择第 3 项“3. Network Menu”后即进入如下所示的“网络”子菜单。该子菜单中的菜单项说明如表 2-14 所示。

```
          Network Menu

      1. Display parameter
      2. Modify parameter
      3. Save parameter
      4. Download file
      5. Upload file
      0. Return

Enter your choice(0-5):
```

表 2-14 网络子菜单的菜单项说明

子菜单项	说明
1. Display parameter	通过此菜单可以查看当前的网络参数
2. Modify parameter	通过管理网口下载或者上传文件之前，需要先通过此菜单设置网络参数。但设置的网络参数仅在当前有效
3. Save parameter	如果要使当前设置的网络参数在系统下次重启时仍然有效，在继续启动设备前，需要先通过此菜单保存网络参数
4. Download file	从服务器下载文件到设备。用户进行了错误的配置，导致功能异常，可以通过此菜单恢复存储器中的配置文件和补丁文件等
5. Upload file	从设备上传文件到服务器。为防止配置信息丢失，可以通过此菜单备份存储器中的配置文件和补丁文件等
0. Return	返回主菜单

下面着重介绍“修改网络参数”（Modify parameter）菜单。进入网络子菜单后选择第 2 项即进入如下所示的修改网络参数菜单。

```
          Network Menu

      1. Display parameter
      2. Modify parameter
      3. Save parameter
      4. Download file
      5. Upload file
```

```
    0. Return

Enter your choice(0-5):2
NOTE:
Ftp type define:   0(ftp), 1(tftp),
ENTER = no change; '.' = clear;

Ftp type                : 0
File name               : cfg.zip
Ethernet ip address : 192.168.1.3
Ethernet ip mask       : ffffff00
Gateway ip address    :
Ftp host ip address : 192.168.1.11
Ftp user                : huawei
Ftp password           : huawei2012

Modify net parameter success.
```

通过此菜单可以设置设备作为 FTP/TFTP 客户端，PC 作为 FTP/TFTP 服务器（需要在 PC 上安装 FTP/TFTP 服务器软件）进行文件的连接参数。在设置网络接口参数时，参数的前、后及中间请不要添加空格；参数仅支持英文字母、阿拉伯数字、下划线和“.”号。

① **Ftp type**：设置设备作为 FTP 客户端或者 TFTP 客户端。0 为 FTP 客户端，1 为 TFTP 客户端。缺省情况下，设备作为 FTP 客户端。

② **File name**：设置需要传输的文件名，可以是系统软件、配置文件或者补丁文件等。

③ **Ethernet ip address**：设置设备的管理口 IP 地址。

④ **Ethernet ip mask**：设置设备的管理口 IP 地址子网掩码。

⑤ **Gateway ip address**：设置设备所在网段的网关地址。

⑥ **Ftp host ip address**：设置担当 TFTP 服务器或者 FTP 服务器的 PC 的 IP 地址。

⑦ **Ftp user**：设置设备上用于访问 FTP 服务器的用户名。

⑧ **Ftp password**：设置设备上用于访问 FTP 服务器的用户密码。

说明 如果设备采用 TFTP 方式传输文件，则 **Ftp user** 和 **Ftp password** 无需设置，直接按 Enter 键。如果设备与服务器属于不同网段，则 **Gateway ip address** 必须设置；若属于同一网段，则 **Gateway ip address** 无需设置。

2.4.5 启动选择子菜单

进入 2.4.2 小节介绍的 BootROM 主菜单，选择第 4 项“4. Startup Select”后即可进入如下所示的“启动选择”（Startup Select）子菜单。该子菜单中的菜单项说明如表 2-15 所示。

```
      Startup Select

     1. Display Startup
     2. Set Boot File
     3. Set Config File
     4. Startupfile Check Manage
     5. Set Startup Waiting Time
     0. return

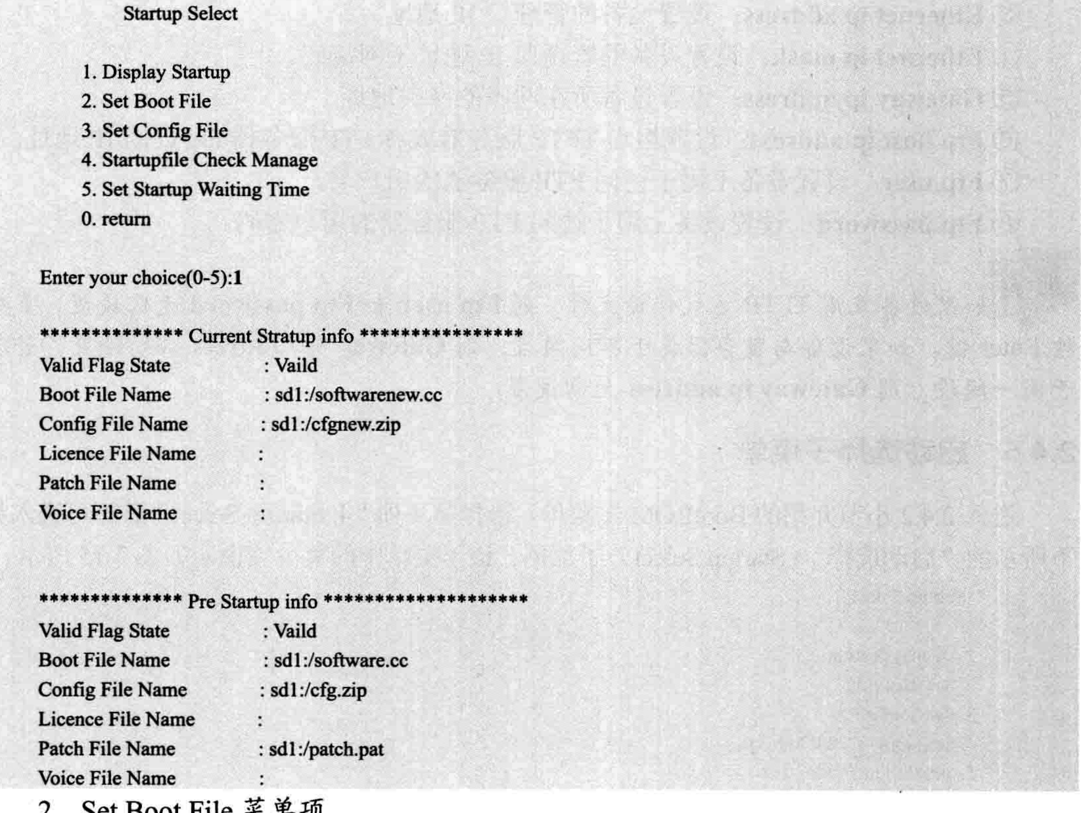
Enter your choice(0-5):
```

表 2-15 启动选择子菜单的菜单项说明

菜单项	说明
1. Display Startup	查看当前启动和前一次启动的系统软件和配置文件等。在系统升级或降级之前，可以通过此菜单查看启动的系统软件及配置文件是否为正确的启动加载文件
2. Set Boot File	设置启动的系统软件。在系统升级或降级之前，需要通过此菜单指定启动时使用的系统软件
3. Set Config File	设置启动的配置文件。在系统升级或降级之前，需要通过此菜单指定启动时使用的配置文件
4. Startupfile Check Manage	启动文件校验管理。当需要查看、修改启动文件校验配置时，需要通过此菜单进行启动文件校验管理
5. Set Startup Waiting Time	设置启动时按下 Ctrl+B 组合键进入 BootROM 主菜单所等待时间。需要输入所需的启动等待时间，时间范围为 3～9 s，缺省时间是 3 s。修改的启动等待时间仅在本次上电的情况下有效，断电重启后则恢复到默认配置的 3 s
0. return	返回主菜单

1. Display Startup 菜单项

进入启动选择子菜单后选择第 1 项后即可进入如下所示的查看启动文件信息菜单。通过此菜单可以查看当前启动信息（Current Stratup info）和前一次启动信息（Pre Startup info）等。当我们想要查看这些信息时，就可以进入到 BootROM 菜单中对应的子菜单中进行操作。



```
        Startup Select

     1. Display Startup
     2. Set Boot File
     3. Set Config File
     4. Startupfile Check Manage
     5. Set Startup Waiting Time
     0. return

Enter your choice(0-5):1

************** Current Stratup info ****************
Valid Flag State          : Vaild
Boot File Name            : sd1:/softwarenew.cc
Config File Name          : sd1:/cfgnew.zip
Licence File Name         :
Patch File Name           :
Voice File Name           :


************** Pre Startup info ********************
Valid Flag State          : Vaild
Boot File Name            : sd1:/software.cc
Config File Name          : sd1:/cfg.zip
Licence File Name         :
Patch File Name           : sd1:/patch.pat
Voice File Name           :
```

2. Set Boot File 菜单项

进入启动选择子菜单，选择第 2 项后即可进入如下所示的设置启动系统软件菜单。

通过该菜单可在系统升级或降级之前，指定启动时使用的系统软件，还可以选择系统软件所在的位置，可以是 Flash、Micro SD 卡或者 U 盘，选择对应的序列号即可。

```
          Startup Select

      1. Display Startup
      2. Set Boot File
      3. Set Config File
      4. Startupfile Check Manage
      5. Set Startup Waiting Time
      0. return

Enter your choice(0-5):2
          Select Boot File    !---选择系统软件所在的存储器

      1. Flash
      2. SDCard[1]
      0. Return

Enter your choice(0-2):2
NOTE: Boot file must be .cc or .CC

Current boot file: sd1:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: sd1:/softwarenew1.cc    !---在这里可以指定新的下次启动所要加载的系统软件
Save the boot file name: sd1:/softwarenew1.cc.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

3. Set Config File 菜单项

进入启动选择子菜单，选择第 3 项后即可进入如下所示的设置配置文件菜单。通过该菜单可以在需要为设备指定满足用户需求的配置文件时，指定启动时使用的配置文件。选择配置文件所在的位置，可以是 Flash、Micro SD 卡或者 U 盘，选择对应的序列号即可。

```
          Startup Select

      1. Display Startup
      2. Set Boot File
      3. Set Config File
      4. Startupfile Check Manage
      5. Set Startup Waiting Time
      0. return

Enter your choice(0-5):3
          Select Config File    !---选择配置文件所在的存储器

      1. Flash
      2. SDCard[1]
      0. Return

Enter your choice(0-2):2
NOTE: Config file must be .zip or .cfg or .ZIP or .CFG

Current Config file: sd1:/cfgnew.zip
Press ENTER directly for no change.
Or, please input the new file name: sd1:/cfgnew1.zip    !---在这里可以指定新的下次启动所要加载的配置文件
```

```
Save the config file name: sd1:/cfgnew1.zip ? Yes or No(Y/N)y
Save load state word...OK!
```

4. Startupfile Check Manage 菜单项

进入启动选择子菜单，选择第4项后即可进入如下所示的启动文件检查菜单。通过该菜单可以在需要查看、修改系统软件校验配置时，进行系统软件校验管理。选择 **1. Set FileCheck Flag** 设置系统软件校验标志位，进行系统软件校验；选择 **2. Clear FileCheck Flag** 取消系统软件校验标志位；选择 **3. Query FileCheck Flag** 查看是否设置系统软件校验标志位。

```
          Startup Select

      1. Display Startup
      2. Set Boot File
      3. Set Config File
      4. Startupfile Check Manage
      5. Set Startup Waiting Time
      0. return

Enter your choice(0-5):4
          File Check Manage

      1. Set FileCheck Flag
      2. Clear FileCheck Flag
      3. Query FileCheck Flag
      0. return
```

2.4.6 文件管理子菜单

进入2.4.2小节介绍的BootROM主菜单，选择第5项“5. File Manager”后即可进入如下所示的“文件管理”（File Manager）子菜单。

```
          File Menu

      1. Flash file system
      2. SDCard file system
      0. Return

Enter your choice(0-2):
```

在文件管理子菜单中选择第1项“1. Flash file system”，即进入如下所示的 **Flash file system** 菜单，管理Flash存储器中的文件。

```
          Flash file system MENU

      1. List file in flash          !---列表 Flash 存储器中的文件
      2. Delete file in flash        !---删除 Flash 存储器中的文件
      3. Rename file in flash        !---重命名 Flash 存储器中的文件
      4. Format Flash file system    !---格式化 Flash 存储器
      0. Return

Enter your choice(0-4):0
```

在文件管理子菜单中选择第2项“2. SDCard file system”，即进入如下所示的 **SDCard file system** 菜单，管理SD卡存储器中的文件。下面具体介绍SD卡文件系统管理菜单中的各个菜单项。前面的几项 **Flash file system** 菜单中的对应菜单项类似。

```
          SDCard file system MENU

        1. List file in SDCard[1]   !---列表 SD 存储器中的文件
        2. Delete file in SDCard[1]    !---删除 SD 存储器中的文件
        3. Rename file in SDCard[1]    !---重命名 SD 存储器中的文件
        4. Format SDCard[1]     !---格式化 SD 存储器
        5. Check SDCard[1]   !---校验 SD 存储器
        0. Return

Enter your choice(0-5):
```

选择第 1 项，进入 **List file in SDCard[1]**菜单，列表显示 SD 卡中的文件。

```
Enter your choice(0-5):1
Files of the device:

drwxrwxrwx           -   Dec 27 2012 07:07:00    logfile
-rwxrwxrwx   77773440    Dec 16 2011 15:18:08    software.cc
-rwxrwxrwx 103661312    Nov 27 2012 19:46:48    softwarenew.cc
-rwxrwxrwx        1241   Mar 03 2012 17:30:34    rootcert.pem
-rwxrwxrwx   86307328    Apr 27 2012 15:11:36    softwarenew1.cc
-rwxrwxrwx        1728   Apr 27 2012 19:21:38    patch.dat
-rwxrwxrwx        3275   Dec 16 2012 07:50:50    cfg.zip
-rwxrwxrwx        2172   Dec 16 2012 14:18:08    cfgnew.zip
-rwxrwxrwx        5414   Dec 17 2012 19:14:26    cfgnew1.zip
-rwxrwxrwx      558320   Sep 18 2012 20:04:10    test.txt
10 files found!
1973735424 Byte total, 1031127040 Byte free.
```

选择第 2 项，进入如下所示的 **Delete file in SDCard[1]**菜单内容，删除要删除的文件。

```
Enter your choice(0-5):2
BE CAREFUL!
This may cause your system fail to start!
Please input the file name you want to delete: test.txt   !---输入要删除的文件
delete it? Yes or No(Y/N): y
Deleting file[sd1:/test.txt], please wait....Done
```

选择第 3 项，进入如下所示的 **Rename file in SDCard[1]**菜单内容，对需要重命名的文件进行重命名。

```
Enter your choice(0-5):3
Please input the file name: cfg.zip          !---输入要重命名的源文件名
Please input the new name: vrpcfg.zip     !---输入新的文件名
Rename file[sd1:/cfg.zip] to [sd1:/vrpcfg.zip], Yes or No(Y/N): y
Rename OK!
```

选择第 4 项，进入如下所示的 **Format SDCard[1]**菜单内容，对 SD 卡进行格式化。但格式化整个启动盘后，启动盘中的所有数据（包括历史系统软件，配置文件等）均会丢失。请谨慎使用！

```
Enter your choice(0-5):4
BE CAREFUL!
All files in the device will be lost.
This may cause your system fail to start!
Are you sure to format it? Yes or No(Y/N): y
Format file system. Please wait....

Format success!
```

选择第 5 项，进入如下所示的 **Check SDCard[1]**菜单内容，校验 SD 卡的合法性。

值为 6 时，仅输出严重等级阈值为 0～6 的信息。

表 2-18 信息的分级

等级阈值	等级名称	描述
0	Emergencies（紧急）	设备发生致命的异常，系统已经无法恢复正常，必须重启设备。如程序异常导致设备重启和内存的使用被检测出错误等
1	Alert（警戒）	设备发生重大的异常，需要立即采取措施。如设备内存占用率达到极限等
2	Critical（危险）	设备发生一般异常，需要采取措施进行处理或原因分析。如设备内存占用率超过低界线、温度超过低温告警线和 BFD 探测出设备不可达等
3	Error（错误）	发生错误的操作或设备的异常流程，不会影响后续业务，但是需要关注并分析原因。如用户的错误指令、用户密码错误和检测出错误协议报文等
4	Warning（警告）	设备运转有些异常点，可能引起业务故障，需要引起注意。如用户关闭路由进程、BFD 探测的一次报文丢失和检测出错误协议报文等
5	Notification（通知）	设备正常运转的关键操作信息。如接口 shutdown、邻居发现和协议状态机的正常跳转等
6	Informational（信息）	设备正常运转的一般性操作信息。如用户使用 display 命令等
7	Debugging（调试）	设备正常运转的一般性信息，用户无需关注

2.5.3 信息的输出

设备产生的信息可以向远程终端、控制台、Log 缓冲区、日志文件、SNMP 代理等方向输出。为了便于各个方向信息的输出控制，信息中心定义了 10 条信息通道，通道之间独立输出，互不影响。用户可以根据需要配置信息的输出规则，控制不同类别、不同等级的信息从不同的信息通道输出到不同的输出方向。缺省情况下，各类信息可以输出的信息通道和输出方向如图 2-5 所示，这些通道的缺省使用说明如表 2-19 所示。

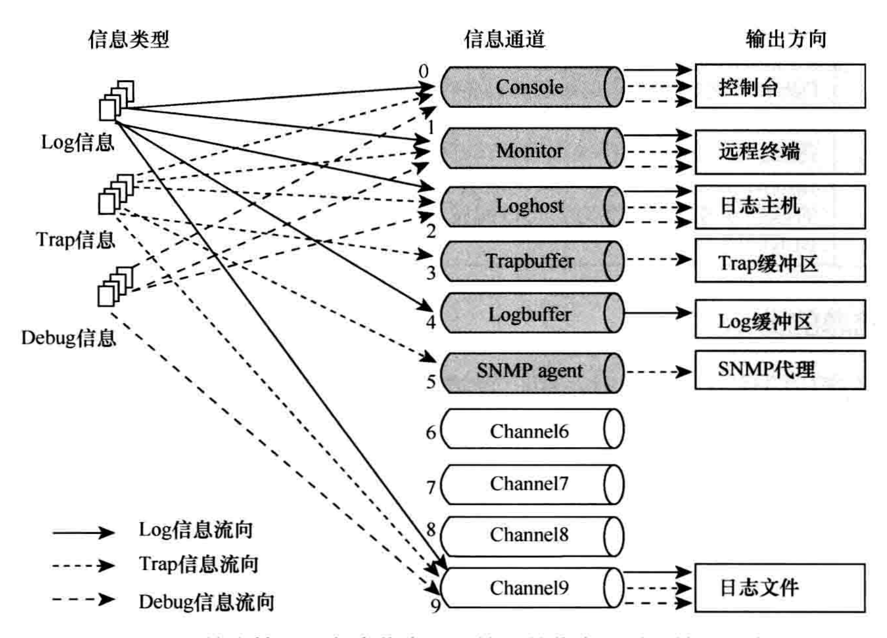


图 2-5 缺省情况下各类信息可以输出的信息通道和输出方向

表 2-16　信息中心的缺省配置

参数	缺省值
信息中心功能	使能
Log 缓冲区容纳 Log 信息的条数	512 条
Trap 缓冲区容纳 Trap 信息的条数	256 条
日志文件大小	8 M
日志文件保存个数	200 个
日志主机 IP 地址	无
时间戳格式	date

2.5.1　信息的分类

根据设备产生信息的不同类别，设备支持对 Log 信息、Trap 信息和 Debug 信息按照不同的输出规则输出到不同的输出方向，具体说明如表 2-17 所示。

表 2-17　三种信息的应用场景及输出方向

信息类别	应用场景	输出方向
Log 信息	Log（日志）信息主要记录用户操作、系统故障、系统安全等信息，包括用户日志和诊断日志。用户通过收集设备产生的 Log 信息，可以实时地了解设备各功能的运行情况，以保证设备的正常工作。当用户需要监控设备的运行状况时，可以配置 Log 信息输出到不同的输出方向	Log 信息支持输出的输出方向有：控制台、远程终端、日志主机、Log 缓冲区和日志文件
Trap 信息	Trap（诱骗）信息是系统检测到故障而产生的通知，主要记录故障等系统状态信息。这类信息不同于 Log 信息，其最大特点是需要及时通知、提醒管理用户，对时间敏感。用户通过收集设备产生的 Trap 信息，可以实时地了解设备的运行情况，及时定位故障信息。可以配置 Trap 信息输出到不同的输出方向	Trap 信息支持输出的输出方向有：控制台、远程终端、日志主机、Trap 缓冲区、SNMP 代理和日志文件
Debug 信息	Debug（调试）信息是系统对设备内部运行的信息的输出，主要用于跟踪设备内部运行的轨迹。只有在设备上打开相应功能模块上的调试开关，设备才能产生相应的 Debug 信息。当用户需要了解设备内部运行的信息或者调试设备时，可以配置 Debug 信息输出到不同的输出方向	Debug 信息支持输出的输出方向有：控制台、远程终端、日志主机和日志文件

2.5.2　信息的分级

当设备产生的信息比较多时，用户较难分辨哪些是设备正常运转的信息，哪些是出现故障需要处理的信息。通过对信息进行分级，用户可以根据信息的级别进行粗略判断，及时采取措施，屏蔽无需处理的信息。

根据信息的严重等级或紧急程度，信息分为 8 个等级，信息越严重，其严重等级阈值（也就是显示的数字）越小。详细的信息分级如表 2-18 所示。

根据严重等级过滤信息时，仅输出严重等级阈值小于或等于所配置的严重等级阈值的信息，即**仅输出等于配置级别和比配置级别更严重的信息**。例如，当配置严重等级阈

```
Enter your choice(0-5):5
Check SD Card[1] file system. Please wait....

                    sd1:/    - Volume is OK

File system check OK!
```

2.4.7 密码管理菜单

进入 2.4.2 小节介绍的 BootROM 主菜单，选择第 7 项“7. Password Manager”后即可进入“密码管理”（Password Manager）子菜单。

```
            PassWord Menu

        1. Modify the menu password
        2. Clear the console login password
        0. Return

Enter your choice(0-2):1
```

选择第 1 项，进入如下所示的 **Modify the menu password** 菜单内容，修改进入 BootROM 主菜单的密码。为了防止非法用户进入 BootROM 菜单，可以通过 **Modify the menu password** 菜单修改进入 BootROM 菜单的密码。

```
Modify password. Press Ctrl+c to break.   !---提示可按 Ctrl+C 组合键中断密码的修改
Enter Old Password:******                 !---输入原来的进入 BootROM 主菜单的密码
Input new password:******                 !---输入新的进入 BootROM 主菜单的密码
Input new password again:******           !---重复输入新的进入 BootROM 主菜单的密码
Are you sure to change password? [y/n]:y
Save new password Success.
```

选择第 2 项，即选择 **Clear the console login password** 菜单项，则立即清除 Console 登录密码（这个密码是在第一次通过 Console 口本地登录时设置的，有的机型也有初始密码，具体参见配套图书《华为交换机学习指南》第 3 章 3.1.1 小节）。清除完成后提示如下清除成功信息。当用户的 Console 口登录密码遗忘导致无法登录设备时，可以通过此菜单项清除。

```
Clear the console login password Succeed!
```

2.5 信息中心基础

AR G3 系列路由器（同时适用于 S 系列交换机）中的信息中心记录了设备运行过程中各个模块产生的信息，包括 Log（日志）、Trap（诱骗）和 Debug（调试）信息。信息中心的缺省配置如表 2-16 所示。

在日常维护设备以及紧急定位故障时，用户或管理员需要及时了解设备运行过程中产生的信息。为了方便及时获取设备信息，可通过配置信息中心，对设备产生的信息按照信息类型、严重级别等进行分类或筛选，还可以灵活地控制信息输出到不同的输出方向（例如控制台、用户终端、日志主机等）。这样，用户或网络管理员可以从不同的地点收集设备产生的信息，方便监控设备运行状态和定位故障。

表 2-19　信息输出通道的缺省使用情况

通道号	缺省通道名	输出方向	输出方向的描述
0	console	控制台	控制台，即通过 Console 口登录设备的方式，可以接收 Log 信息、Trap 信息、Debug 信息
1	monitor	远程终端	远程终端，即通过 VTY 登录设备的方式，可以接收 Log 信息、Trap 信息、Debug 信息，方便远程维护
2	loghost	日志主机	日志主机，可以接收 Log 信息、Trap 信息、Debug 信息。信息在日志主机上以文件形式保存，供随时查看
3	trapbuffer	Trap 缓冲区	Trap 缓冲区，可以接收 Trap 信息
4	logbuffer	Log 缓冲区	Log 缓冲区，可以接收 Log 信息
5	snmpagent	SNMP 代理	SNMP 代理，可以接收 Trap 信息
6	channel6	未指定	保留，可用于分配
7	channel7	未指定	保留，可用于分配
8	channel8	未指定	保留，可用于分配
9	channel9	日志文件	日志文件，可以接收 Log 信息、Trap 信息、Debug 信息 S 系列盒式交换机不支持信息输出到日志文件

缺省情况下，Log 信息、Trap 信息和 Debug 信息都是从图 2-5 所示的缺省信息通道输出的，用户可以根据需要更改信息通道的名称，也可以更改缺省情况下保留的 6、7、8 三个信息通道与输出方向之间的对应关系。例如，用户配置通道 6 的名称为 user1，发往日志主机的信息使用通道 6，则发往日志主机的信息都会从通道 6 输出，不再从通道 2 输出。

2.5.4　信息的输出格式和输出过滤

图 2-6 所示为 Log 信息格式和一条本地存储的日志记录（可通过 **display logbuffer** 命令查看 Log 缓冲区记录的信息，如下所示）所对应的格式各个部分，详细说明如表 2-20 所示。

```
<Huawei> display logbuffer
Logging buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 512
Channel number: 4, Channel name: logbuffer
Dropped messages: 0
Overwritten messages: 167
Current messages: 512

May 10 2012 13:42:59+00:00 huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[0]:Some packets a
```

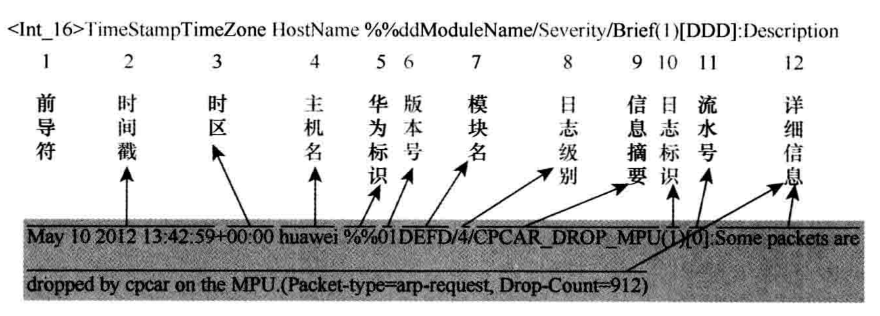


图 2-6　Log 信息的输出格式

```
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-Count=912)
May 10 2012 13:32:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[1]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-Count=684)
May 10 2012 13:22:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[2]:Some packets a
......
```

表 2-20　　Log 信息输出格式的字段说明

字段	字段含义	说明
<Int_16>	前导符	在向日志主机发送信息的时候添加前导符，**在设备本地保存信息时不加前导符**
TimeStamp	时间戳，信息输出的时间	时间戳有 5 种格式可供选择 ● boot 型：指定时间戳采用相对时间类型，即系统启动后经过的时间。格式是 xxxxxx.yyyyyy，xxxxxx 为系统启动后经过时间的毫秒数高 32 位，yyyyyy 为低 32 位 ● date 型：指定时间戳采用系统当前日期和时间。中文环境下为 yyyy/mm/dd hh:mm:ss；英文环境下为 mm dd yyyy hh:mm:ss ● short-date 型：指定时间戳采用短日期格式。这种格式的时间戳与 date 类型的时间戳基本相同，唯一区别是短日期格式取消了年份的显示 ● format-date 型：按照年、月、日、时、分、秒的格式显示：YYYY-MM-DD hh:mm:ss ● none 型：信息中不包含时间戳 Log 信息缺省采用 date 型时间戳
TIMEZONE	本地时区信息	此信息与 **display clock** 命令输出信息中的"Time Zone"字段一致
HostName	主机名	主机名与模块名之间用一个空格隔开
%%	华为公司的标识	标识该 Log 信息是由华为公司的产品输出的
dd	版本号	标识该 Log 信息格式的版本
ModuleName	模块名	向信息中心输出信息的模块名称
Serverity	日志的级别	Log 信息的级别
Brief	简要描述	Log 信息的简要解释
(l)	信息的类别	信息的类型有： ● l：表示为 Log 信息 ● D：表示为诊断日志信息
DDD	日志流水号	也就是日志 ID，序列号。缺省情况下，日志信息可以向控制台、Log 缓冲区、日志文件和 VTY/TTY 终端发送。在 Log 缓冲区中，该值大小取决于 Log 缓冲区的大小。例如，Log 缓冲区的大小为 100，则日志流水号的取值范围是：0～99
Description	描述符	Log 信息的具体内容

图 2-7 所示为 Trap 信息格式以及一条本地存储的 Trap 记录（可通过 **display trapbuffer** 命令查看信息中心 Trap 缓冲区记录的信息，如下所示）对应格式的各个部分，详细说明如表 2-21 所示。

```
<Huawei> display trapbuffer
Trapping buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 256
Channel number: 3, Channel name: trapbuffer
```

```
Dropped messages: 0
Overwritten messages: 0
Current messages: 29

#Sep 17 2012 17:09:47+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 17 2012 17:06:50+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=0, LldpStatsRemTables
Deletes=1, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
......
```

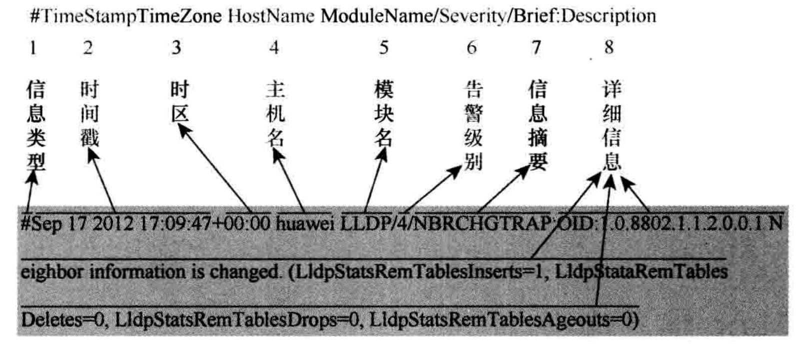


图 2-7　Trap 信息的输出格式

表 2-21　Trap 信息输出格式的字段说明

字段	字段含义	说明
#	信息类型	“#”表示为告警信息，仅在 Trap 缓冲区中存在
TimeStamp	时间戳，信息输出的时间	时间戳有 5 种格式可供选择，参见表 2-21 中 Log 信息输出格式中的该字段说明。Trap 信息缺省采用 date 型时间戳
TIMEZONE	本地时区信息	此信息与 **display clock** 命令输出信息中的“Time Zone”字段一致
HostName	主机名	主机名与模块名之间用一个空格隔开
ModuleName	模块名	向信息中心输出信息的模块名称
Severity	严重级别	Trap 信息的级别
Brief	简要描述	Trap 信息的简要解释
Description	描述信息	Trap 信息的具体内容

为了使信息的输出控制更加灵活，信息中心提供了信息过滤的功能。设备正常运行后，各模块在业务处理时都会上报信息，当用户希望过滤某些不需要关注的业务模块/级别的信息时，可以配置信息在信息通道中的过滤功能。

信息中心通过信息过滤表来实现信息在通道中的过滤。信息过滤表是根据信息分类、分级、来源对输出到各个方向的信息进行过滤的。信息过滤表记录的内容包括信息模块号、Log 信息输出开关状态、Log 信息输出过滤级别、Trap 信息输出开关状态、Trap 信息输出过滤级别、Debug 信息输出开关状态、Debug 信息输出过滤级别，具体将在 2.6、2.7、2.8 节介绍。信息通道的缺省输出规则表定义了不同类别的信息可以输出的信息模块、最低信息级别以及信息通道，如表 2-22 所示。

表 2-22 信息通道的缺省输出规则表

输出通道	允许输出的模块	Log 信息		Trap 信息		Debug 信息	
		使能状态	允许输出最低级别	使能状态	允许输出最低级别	使能状态	允许输出最低级别
0（控制台）	default（所有模块）	使能	warning	使能	debugging	使能	debugging
1（远程终端）	default（所有模块）	使能	warning	使能	debugging	使能	debugging
2（日志主机）	default（所有模块）	使能	informational	使能	debugging	未使能	debugging
3（Trap 缓冲区）	default（所有模块）	未使能	informational	使能	debugging	未使能	debugging
4（Log 缓冲区）	default（所有模块）	使能	warning	未使能	debugging	未使能	debugging
5（SNMP 代理）	default（所有模块）	未使能	debugging	使能	debugging	未使能	debugging
6（channel 6）	default（所有模块）	使能	debugging	使能	debugging	未使能	debugging
7（channel 7）	default（所有模块）	使能	debugging	使能	debugging	未使能	debugging
8（channel 8）	default（所有模块）	使能	debugging	使能	debugging	未使能	debugging
9（channel 9）	default（所有模块）	使能	debugging	使能	debugging	未使能	debugging

2.6 配置 Log 信息输出

可以配置指定模块的 Log 信息输出到 Log 缓冲区、日志文件、控制台、终端和日志主机中，这也就构成了日志信息过滤表。

2.6.1 Log 信息输出配置任务

Log 信息输出所包括的配置任务可以分为两大类：一是 Log 信息输出基本功能和参数配置，二是 Log 信息输出配置。

1. Log 信息输出基本功能和参数配置

Log 信息输出基本功能和参数配置包括以下几个方面（**仅第一项为必选配置任务，**其他均可根据实际需要选择配置，因为它们都有缺省值）。

① 使能信息中心。

只有使能信息中心功能，才能进行信息中心的相关配置。缺省情况下，信息中心功能处于使能状态。



下面的步骤 2～5 为可选步骤，没有严格的配置顺序，可根据实际情况选择配置。

②（可选）命名信息通道。

为了方便记忆和使用，用户可以将各个通道的缺省名称重新命名。

③（可选）配置 Log 信息的过滤功能。

当用户不需要关注某些 Log 信息时，可以配置信息过滤功能来屏蔽此类 Log 信息的输出。

④（可选）配置 Log 信息的时间戳。

如果用户希望为了适应自身习惯或者本地时间而需要调整信息的输出时间格式和时间精度时，可以配置时间戳。

⑤（可选）去使能 Log 信息的计数功能。

如果用户希望记录到日志缓冲区、日志文件或者发送到控制台和终端的日志信息不携带流水号信息，可以配置去使能 Log 信息的计数功能。但通常不配置，因为日志信息中的流水号对于日志信息查看很有帮助。

2. Log 信息输出配置

Log 信息输出可根据实际需要选择以下一种或多种输出方式。

（1）配置 Log 信息输出到 Log 缓冲区

如果用户希望在本地设备的 Log 缓冲区内可以查看到设备产生的 Log 信息，则可以配置 Log 信息输出到 Log 缓冲区。

（2）配置 Log 信息输出到日志文件

如果用户希望把 Log 信息以文件的形式进行保存在本地设备存储器中，便于日后查看，则可配置 Log 信息输出到日志文件。

（3）配置 Log 信息输出到控制台

如果用户希望可以在 Console 控制台上查看到 Log 信息，以便及时监控设备的运行情况，则可以配置 Log 信息输出到控制台。

（4）配置 Log 信息输出到终端

如果用户希望在进行 Telnet 或者 STelnet 的客户端主机上显示 Log 信息，以便及时监控设备的运行情况，则可配置 Log 信息输出到用户终端。

（5）配置 Log 信息输出到日志主机

如果有专门用来存储日志信息的日志主机，且希望把日志信息保存在日志主机上，以便在需要时可以随时查看、及时监控设备的运行情况，则可配置 Log 信息输出到日志主机。

2.6.2 配置 Log 信息输出基本功能

Log 信息输出基本功能配置包括使能信息中心功能，命名信息通道，配置 Log 信息过滤、Log 信息时间戳格式和去使能 Log 信息计数功能这几个方面。具体配置步骤如表 2-23 所示。

表 2-23　Log 信息输出基本功能配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**info-center enable** 例如：[Huawei] **info-center enable**	使能信息中心功能。只有使能了信息中心功能，系统才会向日志主机、控制台等方向输出系统信息 缺省情况下，信息中心功能处于使能状态，可用 **undo info-center enable** 命令去使能信息中心功能。但去使能后，设备上产生的 Log、Trap 和 Debug 信息都不再记录，包括执行 **undo info-center enable** 命令产生的日志信息也不记录

（续表）

步骤	命令	说明
3	**info-center channel** *channel-number* **name** *channel-name* 例如：[Huawei]**info-center channel** 0 **name** execconsole	（可选）为指定编号的信息通道命名。为了方便记忆和使用，用户可以将各个通道重新命名。命令中的参数说明如下 ● *channel-number*：指定通道编号，取值范围为 0～9 的整数，即系统共有 10 个通道 ● *channel-name*：指定通道名称，1～30 个字符，区分大小写，**只能由字母或数字组成，并且首字符只能为字母** 缺省情况下，各信息通道的名称如下：0（console）、1（monitor）、2（loghost）、3（trapbuffer）、4（logbuffer）、5（snmpagent）、6（channel6）、7（channel7）、8（channel8）、9（channel9），可用 **undo info-center channel** *channel-number* 命令恢复指定通道为缺省的通道名
4	**info-center filter-id** { *id* | **bymodule-alias** *modname alias* } * &<1-50> 例如：[Huawei] **info-center filter-id bymodule-alias** CMD CLKCHGREBOOTCANCELED	（可选）配置对指定的 Log 信息进行过滤的功能。命令中的参数说明如下 ● *id*：可多选参数，指定需要过滤的 Log 信息对应的 ID 信息（**即日志序列号**），为系统中显示的日志 ID，取值范围为 0～4 294 967 295 的整数 ● **bymodule-alias** *modname alias*：可多选参数，指定需要过滤的 Log 信息对应的模块名称和助记符名称，要根据日志中的提示选取 ● &<1-50>：表示前面的 *id* | **bymodule-alias** *modname alias* 参数最多可配置 50 个，中间以空格分隔 缺省情况下，不对任何 Log 或 Trap 信息进行过滤，可用 **undo info-center filter-id** { **all** | { *id* | **bymodule-alias** *modname alias* } * &<1-50> }命令取消对指定或者所有的 Log 信息进行过滤的功能
5	**info-center timestamp log** { { **date** | **short-date** | **format-date** } [**precision-time** { **tenth-second** | **millisecond** }] | **boot** | **none** } 例如：[Huawei] **info-center timestamp log date precision-time millisecond**	（可选）配置输出的 Log 信息的时间戳格式。命令中的选项说明如下 ● **date**：多选一选项，指定时间戳采用系统当前日期和时间，格式为 mm dd yyyy hh:mm:ss ● **short-date**：多选一选项，指定时间戳采用短日期格式。这种格式的时间戳与 **date** 类型的时间戳基本相同，唯一区别是短日期格式取消了年份的显示，为 mm dd hh:mm:ss ● **format-date**：多选一选项，按照年、月、日、时、分、秒的格式显示：YYYY-MM-DD hh:mm:ss ● **precision-time**：可选项，指定时间戳精度 ● **tenth-second**：二选一可选项，指定时间戳精确到 0.1 s ● **millisecond**：二选一可选项，指定时间戳精确到毫秒 ● **boot**：多选一选项，指定时间戳采用相对时间类型，即系统启动后经过的时间。格式是 xxxxxx.yyyyyy，xxxxxx 为系统启动后经过时间的毫秒数高 32 位，yyyyyy 为低 32 位 ● **none**：多选一选项，指定输出的信息不包含时间戳 缺省情况下，Log 信息采用的时间戳格式为 **date**，可用 **undo info-center timestamp log** 命令恢复输出的 Log 信息的时间戳格式为缺省值

（续表）

步骤	命令	说明
6	**info-center local log-counter disable** 例如：[Huawei] **info-center local log-counter disable**	（可选）去使能日志信息计数功能。如果用户希望记录到日志缓冲区、日志文件或者发送到控制台和终端的 Log 信息不携带流水号（也即日志信息的序列号）信息，可以配置去使能 Log 信息的计数功能 缺省情况下，本地日志信息计数功能处于使能状态，可用 **undo info-center local log-counter disable** 命令使能本地日志信息计数功能 【说明】如果用户希望这些记录到日志缓冲区、日志文件或者发送到控制台和终端的日志信息重新计数，或者，如果用户为了查看是否所有的日志信息都记录到日志缓冲区、日志文件或者发送到控制台和终端，可以使用 **undo info-center local log-counter disable** 命令打开日志计数功能，使生成的日志带有顺序递增的序列号 如果日志发送到、日志文件控制台或者终端，则日志信息在这些不同的输出方向上独立计数，**日志计数序列号为正向排序，即最早的日志计数序列号为 0，越新的日志序列号越大；而如果日志发送到日志缓冲区，那么日志计数序列号为逆向排序，即最新的日志计数序列号为 0，越老的日志序列号越大**

2.6.3 配置 Log 信息输出到 Log 缓冲区

如果用户希望可通过 **display logbuffer** 命令查看在 Log 缓冲区内设备产生的 Log 信息，可以配置 Log 信息输出到 Log 缓冲区。具体的配置步骤如表 2-24 所示（**需要事先配置好 2.6.2 小节介绍的基本功能和参数**）。

表 2-24　配置 Log 信息输出到 Log 缓冲区的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**info-center logbuffer** 例如：[Huawei] **info-center logbuffer**	使能 Log 信息向 Log 缓冲区的发送功能 缺省情况下，Log 信息向 Log 缓冲区的发送功能处于使能状态，可用 **undo info-center logbuffer** 命令去使能 Log 信息向 Log 缓冲区的发送功能
3	**info-center logbuffer channel** { *channel-number* | *channel-name* } 例如：[Huawei] **info-center logbuffer hannel** 3	配置 Log 信息输出到 Log 缓存区所使用的通道。命令中参数说明如下 • *channel-number*：二选一参数，指定输出的通道编号 • *channel-name*：二选一参数，指定输出的通道名称 缺省情况下，系统向 Log 缓冲区输出信息使用 4 号通道，可用 **undo info-center logbuffer channel** { *channel-number* | *channel-name* }命令恢复为缺省情况
4	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* } *	配置向信息通道输出 Log 信息的规则。命令中的参数和选项说明如下 • *module-name*：多选一参数，指定要配置输出 Log 信息规则的模块名，根据系统中模块注册信息选取 • **default**：指定为缺省模块配置输出 Log 信息规则

（续表）

步骤	命令	说明
4	例如：[Huawei]**info-center source** CFM **channel** snmpagent **log level warning**	• *channel-number*：二选一参数，指定要配置规则的输出的通道编号 • *channel-name*：二选一参数，指定要配置规则的输出的通道名称 • **log** { **state** { **off** | **on** }}：可多选选项，指定 Log 信息的发送状态，**off**：不发送 Log 信息，**on**：发送 Log 信息 • **log** { **level** *severity* }：可多选参数，指定 Log 信息允许输出的最低信息级别。信息中心按信息的严重等级或紧急程度划分为 8 个级别，级别从高到低分别为：emergencies→alert→ critical→error→warning→notification→informational→debugging 缺省情况下，系统向 4 号通道输出 Log 信息的状态为 **on**，最低信息级别为 **warning**，**可用 undo info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }命令恢复指定信息通道输出信息的规则为缺省值
5	**info-center logbuffer size** *logbuffer-size* 例如：[Huawei] **info-center logbuffer size** 500	配置 Log 缓冲区可容纳 Log 信息的条数。参数 *logbuffer-size* 用来指定 Log 缓冲区可容纳 Log 消息的条数，取值范围为 0～1 024 的整数。如果设置为 0，表示 Log 信息不显示 【说明】当 Log 缓冲区的 Log 信息数目已经达到最大的 Log 缓冲区尺寸时，就会按照时间的顺序对进入 Log 缓冲区中的时间最早的 Log 信息进行覆盖，直到满足新 Log 信息的存放为止。除非设备重启，否则，Log 缓冲区的 Log 信息不会被清空 本命令为覆盖式命令，多次执行该命令后，Log 信息显示的条数按照最后一次配置生效 缺省情况下，Log 缓冲区可容纳日志信息的数目为 512 条，可用 **undo info-center logbuffer size** 命令恢复 Log 缓冲区可容纳 Log 信息的条数为缺省值

2.6.4 配置 Log 信息输出到日志文件

日志信息可以以文件的形式保存在设备上，便于用户随时查看设备的运行情况。但仅当设备中存在存储介质（例如，U 盘或 SD 卡等）时，日志信息才能以日志文件的形式保存。配置 Log 信息输出到日志文件的步骤如表 2-25 所示（**需要事先配置好 2.6.2 小节介绍的基本功能和参数**）。

表 2-25　　配置 Log 信息输出到日志文件的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**info-center logfile channel** { *channel-number* | *channel-name* } 例如：[Huawei] **info-center logbuffer channel** 3	配置 Log 信息输出到日志文件所使用的通道。命令中参数说明参见 2.6.3 小节表 2-24 中的第 3 步 缺省情况下，系统向日志文件输出信息使用 9 号通道，可用 **undo info-center logfile channel** { *channel-number* | *channel-name* }命令恢复为缺省情况

（续表）

步骤	命令	说明
3	**info-center source** { *module-name* | default } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* }* 例如：[Huawei]**info-center source** CFM **channel** snmpagent **log level warning**	配置向信息通道输出 Log 信息的规则。命令中的参数和选项说明参见 2.6.3 小节表 2-24 中的第 4 步
4	**info-center logfile path** *path* 例如：[Huawei] **info-center logfile path** usb0:**/logfile**	（可选）配置日志文件保存的路径。参数 *path* 用来指定日志文件保存的路径，路径格式为：存储介质:/logfile/（如 usb0:/logfile/），日志文件名为 log.log。但不同 AR G3 系列路由器可选择的存储设备不一样，具体如下 ● 对于 AR150/150-S/160/200/200-S 系列，以及 AR2201-48FE-S、AR2204-S、AR2201-48FE、AR2202-48FE、AR2204、AR2220L，缺省情况下，日志文件存储介质为 Flash ● 对于 AR1200/1200-S 系列，缺省情况下，日志文件存储介质为 usb0。如果设备中没有插入 usb0，则选择 usb1。如果设备中没有插入 usb0 和 usb1，则选择 Flash。如果设备中不存在 usb0、usb1 和 Flash，则不能保存日志文件 ● 对于 AR2220、AR2220-S、AR2240-S、AR2240 和 AR3200 系列，存储介质按照 sd0、sd1、usb0 和 usb1 的优先级顺序进行选择。缺省情况下，日志文件存储介质为 sd0。如果设备中没有插入 sd0，则选择路径 sd1，依此类推。如果设备中不存在 sd0、sd1、usb0 和 usb1，则不能保存日志文件
5	**info-center logfile size** *size* 例如：[Huawei] **info-center logfile size** 32	（可选）配置日志文件的大小。参数 *size* 用来指定日志文件的大小，取值可以是 4、8、16 和 32，单位是 MB 【说明】当配置日志信息输出到日志文件方向时，产生的日志文件先保存到 log.log 文本格式中，超过指定大小后，自动按照标准 zip 格式压缩成压缩文件。当剩余设备存储空间小于 100 MB 时，信息中心会删除保存时间最长的一个日志文件 缺省情况下，日志文件的大小为 8 MB，可用 **undo info-center logfile size** 命令恢复日志文件的大小为缺省值
6	**info-center max-logfile-number** *filenumbers* 例如：[Huawei] **info-center max-logfile-number** 100	（可选）配置日志文件的最大保存个数。参数 *filenumbers* 用来指定保存日志文件的最大个数，取值范围为 2～500 的整数 【说明】配置日志文件的最大保存个数以后，如果产生的日志文件超过最大个数，系统将删除日期较老的日志文件（也可手动删除指定的日志文件），保持日志文件个数小于等于所配置的值 缺省情况下，日志文件的最大保存个数为 200，可用 **undo info-center max-logfile-number** 命令恢复日志文件的最大保存个数为缺省值

2.6.5 配置 Log 信息输出到控制台或终端

通过配置 Log 信息输出到控制台，用户可以在 Console 控制台（通过 Console 口登录到设备上的主机）上看到 Log 信息，以便及时监控设备的运行情况；通过配置 Log 信息输出到用户终端，Telnet 或者 STelnet 用户可以在终端 PC（通过 Telnet 或者 STelnet 等方式登录到设备上的主机）上看到 Log 信息，以便及时监控设备的运行情况。

本节的配置步骤与上节的基本一样，唯一的区别在于信息通道使用的配置上。具体的配置步骤如表 2-26 所示（**需要事先配置好 2.6.2 小节介绍的基本功能和参数**）。

表 2-26 配置 Log 信息输出到控制台或终端的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**info-center** { **console** | **monitor** } **channel** { *channel-number* | *channel-name* } 例如：[Huawei] **info-center logbuffer channel** 3	配置 Log 信息输出到控制台（选择 **console** 二选一选项时）或者终端（选择 **monitor** 二选一选项时）所使用的通道。命令中参数说明参见 2.6.3 节表 2-24 中的第 3 步 缺省情况下，系统向控制台输出信息使用 0 号通道，系统向终端输出信息使用 1 号通道，可用 **undo info-center** { **console** | **monitor** } **channel** { *channel-number* | *channel-name* }命令恢复 Log 信息输出到控制台或者终端时使用缺省通道
3	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } log { **state** { **off** | **on** } | **level** *severity* } * 例如：[Huawei]**info-center source** CFM **channel** snmpagent **log level warning**	配置向信息通道输出 Log 信息的规则。命令中的参数和选项说明参见 2.6.3 节表 2-24 中的第 4 步
4	**quit** 例如：[Huawei] **quit**	退出系统视图，返回用户视图
5	**terminal monitor** 例如：<Huawei> **undo terminal monitor**	使能终端显示信息中心发送的信息的功能（**只影响输入该命令的当前终端**）。这里只是总体上打开在终端上显示信息的开关，要在本终端上显示 Log 信息（还可显示 Trap 和 Debug 信息），还需要配置下一步 缺省情况下，控制台显示信息中心发送的信息的功能处于使能状态（**所以在控制台上显示信息中心发送的信息的功能是不需要另外配置的**），但用户终端显示信息中心发送的信息的功能处于未使能状态，可用 **undo terminal monitor** 命令去使能控制台，或终端显示信息中心发送的信息的功能。执行 **undo terminal monitor** 命令取消显示功能时，相当于执行 **undo terminal debugging**，**undo terminal logging**，**undo terminal trapping** 命令，所有的 Debug/Log/Trap 信息在本终端都不显示
6	**terminal logging** 例如：<Huawei> **undo terminal logging**	使能控制台、终端显示 Log 信息功能。如果希望在终端看到系统的 Log 信息时，可以使用本命令使能终端显示 Log 信息功能 缺省情况下，控制台、终端显示 Log 信息功能处于使能状态，可用 **undo terminal logging** 命令去使能控制台或终端显示 Log 信息的功能

2.6.6 配置 Log 信息输出到日志主机

当用户需要监控的设备不在本地，且需要查询该设备产生的信息时，可以在该设备上配置信息输出到日志主机，以便用户在日志主机侧接收设备产生的信息。具体配置步骤如表 2-27 所示（**需要事先配置好 2.6.2 小节介绍的基本功能和参数**）。

表 2-27　配置 Log 信息输出到日志主机的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] } | { **vpn-instance** *vpn-instance-name* | **public-net** }] * 例如：[Huawei] **info-center loghost** 10.1.1.1 **binary** 3000	配置向日志主机输出信息。命令中的参数和选项说明如下 ● *ip-address*：指定日志主机的 IP 地址 ● **channel** { *channel-number*| *channel-name* }：可多选参数，指定向日志主机发送信息所使用的信息通道号或通道名称。当用户希望发送到不同的日志主机使用不同的通道时，可以通过配置信息输出的信息通道来实现。如使向 IP 为 192.138.0.1 的日志主机发送信息采用通道 7，向 IP 为 192.138.0.2 的日志主机发送信息采用通道 8。 ● **facility** *local-number*：可多选参数，指定设置日志主机的记录工具，取值范围为 loca10～loca17。缺省值是 loca17 ● **language** *language-name*：二选一参数，指定信息输出到日志主机所显示的语言模式，目前仅支持英语模式，即 English ● **binary**：二选一选项，指定向日志主机发送二进制形式的日志 ● *port*：可选参数，指定发送信息时所用的端口号，取值范围为 1～65 535 的整数，缺省值为 514 ● **vpn-instance** *vpn-instance-name*：二选一参数，指定日志主机所在的 VPN 实例的名称，1～31 个字符，不支持空格，**区分大小写** ● **public-net**：二选一选项，指定在公共网络中连接日志主机 最多可以配置 8 个日志主机，实现日志主机间相互备份的功能 缺省情况下，不向日志主机输出信息，可用 **undo info-center loghost** *ip-address* [**vpn-instance** *vpn-instance-name*] 命令取消向日志主机输出信息
3	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* } * 例如：[Huawei]**info-center source** CFM **channel** snmpagent **log level warning**	配置向信息通道输出 Log 信息的规则。命令中的参数和选项说明参见 2.6.3 小节表 2-24 中的第 4 步
4	**info-center loghost source** *interface-type interface-number* 例如：[Huawei] **info-center loghost source** loopback 0	配置设备向日志主机发送消息的源接口信息（可以是物理接口，也可以是逻辑接口）。如果多台设备向同一个日志主机发送信息，通过对不同的设备设置不同的源接口，就可以通过源接口地址判断日志消息是从哪台设备发出的，从而便于对收到的日志消息检索。当然，要确保源接口与日志主机之间路由可达 缺省情况下，从一台设备发出日志消息时，源接口是发送消息的接口，可用 **undo info-center loghost source** 命令恢复设备向日志主机发送消息的源接口信息为缺省值

2.6.7 Log 信息输出管理

配置好以上各节 Log 信息输出后，可用以下 **display** 任意视图命令查看相关配置信息，验证配置结果，也可以使用以下用户视图命令清除相关 Log 信息统计。

① **display info-center**：查看信息中心输出方向的配置信息。

② **display info-center statistics**：查看信息中心的统计信息。

③ **display channel** [*channel-number* | *channel-name*]：查看指定或所有信息通道的配置信息。

④ **display info-center filter-id** [*id* | **bymodule-alias** *modname alias*]：查看信息中心过滤的指定流水号或者模块的信息。

⑤ **display info-center logfile path**：查看日志文件保存的路径。

⑥ **display logfile** *file-name* [*offset* | **hex**] *：查看指定文件名的整个或者指定偏移量的日志文件信息。

⑦ **display logbuffer**：查看 Log 缓冲区记录的信息。

⑧ **reset info-center statistics**：清除各模块的信息统计数据。

⑨ **reset logbuffer**：清除 Log 缓冲区中的日志信息。

2.6.8 向日志文件输出 Log 信息的配置示例

本示例的基本拓扑结构如图 2-8 所示，RouterA 通过网络与 FTP Server 相连且路由可达。网络维护人员希望在 FTP Server 上查看 RouterA 上产生的日志信息，以了解 RouterA 的运行情况。

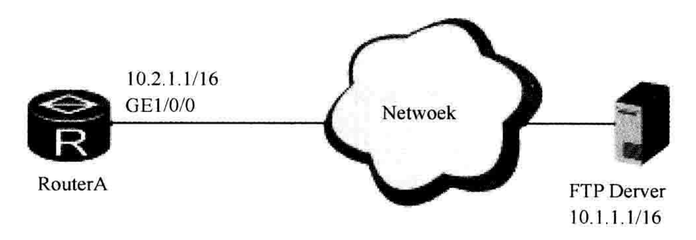


图 2-8 向日志文件输出 Log 信息配置示例拓扑结构

1. 基本配置思路分析

这是一个把日志信息生成文件并发送到远程主机的配置示例，可在 RouterA 上直接根据 2.6.1 小节和 2.6.4 小节介绍的配置方法配置以下基本任务。

① 使能信息中心。

② 配置向日志文件发送 Log 信息的信息通道和输出规则，以实现设备产生的 Log 信息以日志文件的形式保存的目的。

③ 配置日志文件发送到 FTP Server，以实现网络管理员能够在 FTP Server 上查看 RouterA 上产生的日志信息的目的。

2. 具体配置步骤

① 使能信息中心功能。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] info-center enable
```

② 配置向日志文件发送 Log 信息的信息通道和输出规则。假设使用未分配的 6 号通道用于 Log 信息向日志文件发送（参见 2.5.3 节的图 2-5，缺省情况下，输出到日志文件所使用的信息通道为 9 号通道。如果使用缺省通道，则可不配置信息通道），允许向日志文件发送的 Log 信息的最低信息级别为 **warning**（缺省情况下，最低信息级别为 **debugging**）。

```
[RouterA] info-center logfile channel channel6
[RouterA] info-center source ip channel channel6 log level warning
```

③ 配置日志文件传输到 FTP Server。首先要配置从 RouterA 上登录到 FTP Server，假设 FTP Server 的用户名为 huawei，密码为 huawei。

```
<RouterA> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(10.1.1.1:(none)):huawei
331 Give me your password, please
Enter password:
230 Logged in successfully
```

然后将设备生成的日志文件传输到 FTP Server。

```
[RouterA-ftp] put sd1:/logfile/log.log
200 PORT command okay
150 "D:\UPDATE\log.log" file ready to receive in ASCII mode
226 Transfer finished successfully.
FTP: 2761463 byte(s) sent in 26.062 second(s) 105.95Kbyte(s)/sec.
[RouterA-ftp] quit
```

上传好后，可以通过 **display info-center** 命令查看日志文件通道记录的信息发送和接收情况。

```
<RouterA> display info-center
Information Center: enabled
Log host:
Console:
        channel number: 0, channel name: console
Monitor:
        channel number: 1, channel name: monitor
SNMP Agent:
        channel number: 5, channel name: snmpagent
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 204, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 256, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 29
Logfile:
        channel number: 6, channel name: channel6, language: English
```

```
Information timestamp setting:
        log - date, trap - date, debug - date

Sent messages = 1514, Received messages = 1514
```

也可在 FTP 服务器端查看传送到的日志文件。

2.6.9 向日志主机输出 Log 信息的配置示例

本示例的基本拓扑结构如图 2-9 所示，Router 分别与 4 个日志主机相连且路由可达。网络管理员希望不同的日志主机接收不同类型和严重级别的 Log 信息，同时，希望能够保证日志主机接收 Log 信息的可靠性，以便对设备不同模块产生的信息进行实时监控。

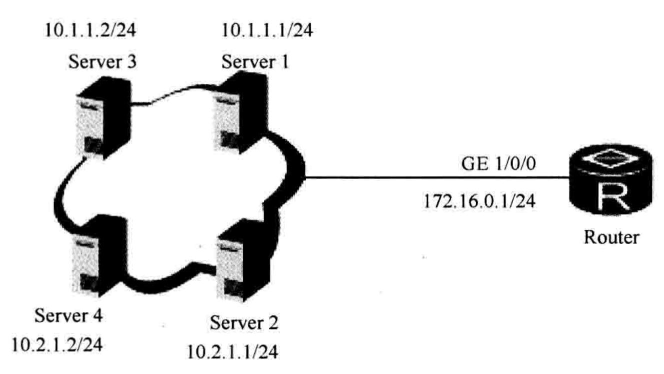


图 2-9 向日志主机输出 Log 信息配置示例拓扑结构

1. 基本配置思路分析

根据本示例要求，可以采用如下配置思路实现示例要求。

① 使能信息中心功能。

② 配置 Router 向日志主机 Server1 发送由 FIB 模块和 IP 模块产生的、严重等级为 notification 的 Log 信息；Router 向日志主机 Server2 发送由 PPP 模块和 AAA 模块产生的、严重等级为 warning 的 Log 信息。另外，为了保证日志主机的可靠性，可配置 Server3 作为 Server1 的备份设备；Server4 作为 Server2 的备份设备。

③ 在 4 台 Server 上配置日志主机，以实现网络管理员能够在日志主机上接收 Router 产生的 Log 信息。

2. 具体配置步骤

① 使能信息中心功能。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] info-center enable
```

② 配置向日志主机发送 Log 信息的信息通道和输出规则。

为了便于以后识别，首先对要用的信息通道进行重命名。现假设 4 台 Server（两台一组）日志主机要用到 6 号和 7 号信息通道，并且分别重命名为 loghost1 和 loghost2。

```
[Router] info-center channel 6 name loghost1
[Router] info-center channel 7 name loghost2
```

然后配置 4 台 Server 日志主机所用的以上重命名的两个信息通道，Server1 和 Server3 使用名为 loghost1 的通道，Server2 和 Server4 使用名为 loghost2 的通道。

```
[Router] info-center loghost 10.1.1.1 channel loghost1
[Router] info-center loghost 10.2.1.1 channel loghost2
[Router] info-center loghost 10.1.1.2 channel loghost1
[Router] info-center loghost 10.2.1.2 channel loghost2
```

再配置向日志主机通道输出 Log 信息的规则。向 Server1 和 Server3 发送 FIB 模块和 IP 模块产生的、严重等级为 notification 的 Log 信息，向 Server2 和 Server4 发送 PPP 模块和 AAA 模块产生的、严重等级为 warning 的 Log 信息。

```
[Router] info-center source fib channel loghost1 log level notification
[Router] info-center source ip channel loghost1 log level notification
[Router] info-center source ppp channel loghost2 log level warning
[Router] info-center source aaa channel loghost2 log level warning
```

③ 配置发送 Log 信息的源接口。

```
[Router] info-center loghost source gigabitethernet 1/0/0
```

最后，还需在 Server 端配置日志主机。日志主机可以是安装 UNIX 或 LINUX 操作系统的主机，也可以是安装第三方日志软件的主机，具体配置步骤请参见相关手册。

配置好后可以通过 **display info-center** 命令查看已经配置的日志主机信息。

```
<Router> display info-center
Information Center: enabled
Log host:
        the interface name of the source address:GigabitEthernet1/0/0
        10.1.1.1, channel number: 6, channel name: loghost1
        language: english, host facility: local7
        10.2.1.1, channel number: 7, channel name: loghost2
        language: english, host facility: local7
        10.1.1.2, channel number: 6, channel name: loghost1
        language: english, host facility: local7
        10.2.1.2, channel number: 7, channel name: loghost2
        language: english, host facility: local7
Console:
         channel number : 0, channel name : console
Monitor:
         channel number : 1, channel name : monitor
SNMP Agent:
         channel number : 5, channel name : snmpagent
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 218, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 256, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 150
Logfile:
        channel number: 9, channel name: channel9, language: English
Information timestamp setting:
         log - date, trap - date, debug - boot

 Sent messages = 683, Received messages = 682
```

可在网管端查看接收到的 Log 信息（略）。

2.7 配置 Trap 信息输出

配置 Trap 信息的输出与上节介绍的 Log 信息输出的配置总体上差不多，也可以配置指定模块的 Trap 信息输出到 Trap 缓冲区、日志文件、控制台、终端、日志主机和 SNMP 代理中。

2.7.1 Trap 信息输出配置任务

从整体上来说，Trap 信息输出包括的配置任务可以分为两大类：一是 Trap 信息输出基本功能和参数配置，二是 Trap 信息输出配置。

1. Trap 信息输出基本功能和参数配置

Trap 信息输出基本功能和参数配置包括以下几个方面，**与 2.6.2 小节表 2-23 中第 2～5 步的对应配置方法基本一样**，只是要在第 5 步配置时间戳格式的命令中把"**log**"关键字要替换成"**tarp**"（整条命令为 **info-center timestamp trap** {{ **date** | **short-date** | **format-date** } [**precision-time** { **tenth-second** | **millisecond** }] | **boot** |**none** }）。

① 使能信息中心。

②（可选）命名信息通道。

③（可选）配置 Trap 信息的过滤功能。

④（可选）配置 Trap 信息的时间戳。

2. Trap 信息输出配置

Trap 信息的输出方式与 2.6 节介绍的 Log 信息输出相比，多了一个可以输出到 SNMP 代理，具体如下。前面几种输出方式的配置方法与 2.6 节介绍的对应 Log 信息输出方式的配置方法是完全或者基本一致的。

（1）配置 Trap 信息输出到 Trap 缓冲区

本项配置任务与 2.6.3 小节表 2-24 介绍的 Log 信息输出到 Log 缓冲区的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **trap**，**logbuffer** 关键字替换为 **trapbuffer**，参数 *logbuffer-size* 对应替换为 *trapbuffer-size*；另外，在缺省情况下，系统向 Trap 缓冲区输出信息使用 3 号通道（向 Log 缓冲区输出信息使用的是 4 号通道）；缺省情况下，系统向 3 号通道输出 Trap 信息的状态为 **on**，最低信息级别为 **debugging**（系统向 4 号通道输出 Log 信息的最低信息级别为 **warning**）。这里配置的是 Trap 信息输出到 Trap 缓冲区。

（2）配置 Trap 信息输出到日志文件

本项配置任务与 2.6.4 小节表 2-25 介绍的 Log 信息输出到日志文件的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **trap**，且这里配置的是 Trap 信息输出到日志文件。

（3）配置 Trap 信息输出到控制台或终端

这两项配置任务的配置方法与 2.6.6 小节表 2-24 介绍的 Log 信息输出控制台和输出到终端的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **trap**；另外，在缺省情况下，系统向 0 号（控制台）或者 1 号（终端）通道输出 Trap 信息的状态为

on，最低信息级别为 **debugging**（Log 信息的最低信息级别为 **warning**），且这里配置的是 Trap 信息输出到控制台或终端。

（4）配置 Trap 信息输出到日志主机

本项配置任务与 2.6.7 小节表 2-25 介绍的 Log 信息输出到日志主机的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **trap**；另外，在缺省情况下，系统向 2 号通道输出 Trap 信息的状态为 **on**，最低信息级别为 **debugging**（Log 信息的最低信息级别为 **informational**）。

（5）配置 Trap 信息输出到 SNMP 代理

当设备出现异常或故障时，网络管理员希望能及时了解设备的运行情况，以保证设备的正常工作。通过配置 Trap 信息输出到网管服务器，可以实现网络管理员对设备的实时监控，及时定位设备运行故障。配置 Trap 信息输出到网管之前，需要先配置 Trap 信息输出到 SNMP 代理，然后通过 SNMP 代理向网管服务器发送 Trap 信息。

下面仅介绍与 Trap 信息输出到 SNMP 代理的配置方法。

2.7.2　配置 Trap 信息输出到 SNMP 代理

Trap 信息输出的具体配置步骤如表 2-28 所示。

表 2-28　　配置 Trap 信息输出到 SNMP 代理的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**info-center snmp channel** { *channel- number* | *channel-name* } 例如：[Huawei] **info-center trapbuffer channel** 5	配置 Trap 信息输出到 SNMP 代理所使用的通道。命令中的参数说明参见 2.6.3 小节表 2-24 中的第 3 步 缺省情况下，系统向 SNMP 代理输出信息使用 5 号通道，可用 **undo info-center snmp channel** { *channel-number* | *channel-name* }命令恢复为缺省
3	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* } * 例如：[Huawei]**info-center source** CFM **channel** snmpagent **log level warning**	配置向信息通道输出 Trap 信息的规则。命令中的参数及其他说明参见 2.6.3 小节表 2-24 中的第 4 步
4	**snmp-agent** 例如：[Huawei] **snmp-agent**	使能 SNMP 代理 缺省情况下，未使能 SNMP 代理功能，可用 **undo snmp-agent** 命令去使能 SNMP 代理功能，但执行 **undo snmp-agent** 命令会使设备上所有 SNMP 版本（SNMPv1，SNMPv2c，SNMPv3）设置失效

说明　配置好以上 Trap 信息输出后，除了可以使用 2.6.7 小节介绍的 **display info-center**、**display info-center statistics**、**display channel** [*channel-number* | *channel-name*]、**display info-center filter-id** [*id* | **bymodule-alias** *modname alias*]、**display info-center logfile path**、**display logfile** *file-name* [*offset* | **hex**] * 命令外，还可使用 display trapbuffer [size *value*]查看信息中心 Trap 缓冲区记录的信息；使用 **reset trapbuffer** 命令清除 Trap 缓冲区中的 Trap 信息。

2.7.3 向 SNMP 代理输出 Trap 信息的配置示例

本示例的基本拓扑结构如图 2-10 所示，Router 与网管站相连且路由可达。网络管理员希望在网管站查看 Router 产生的 Trap 信息，以便监控设备运行情况及定位故障信息。

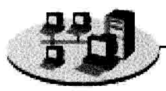




图 2-10 向 SNMP Agent 输出 Trap 信息配置示例拓扑结构

1. 基本配置思路分析

本示例可以直接采用 2.7.1 小节中介绍的 Trap 信息输出基本功能配置和 2.7.2 小节介绍的 SNMP 代理输出方式的配置方法进行配置。基本配置思路如下。

① 使能信息中心功能。

② 配置向 SNMP 代理输出 Trap 信息的信息通道和输出规则，以实现 Router 产生的 Trap 信息发往 SNMP 代理方向。

③ 配置 Trap 信息输出到网管站，以实现网络管理员能够在网管站接收 Router 产生的 Trap 信息。

2. 具体配置步骤

① 使能信息中心功能。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] info-center enable
```

② 配置向 SNMP 代理发送 Trap 信息的信息通道和输出规则：假设使用信息通道 7，允许发送 IP 模块的 Trap 信息的级别为 **informational**。

```
[Router] info-center snmp channel channel7
[Router] info-center source ip channel channel7 trap level informational state on
```

③ 配置 SNMP 代理输出 Trap 信息到网管站。

首先使能 SNMP 代理功能，配置版本为 SNMPv2c。

```
[Router] snmp-agent sys-info version v2c
```

然后配置设备读写团体名。

```
[Router] snmp-agent community write huawei
```

最后配置 SNMP 代理的 Trap 功能。

```
[Router] snmp-agent trap enable
Info: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[Router] snmp-agent target-host trap-hostname nms address 10.1.1.1 trap-paramsname trapnms
[Router] snmp-agent target-host trap-paramsname trapnms v2c securityname public
[Router] quit
```

配置好后，可以使用 **display info-center** 命令查看 SNMP Agent 输出信息所使用的通道。

```
<Router> display info-center
Information Center: enabled
Log host:
        10.1.1.6, channel number: 2, channel name: loghost
        language: english, host facility: local7
        binary loghost, port number: 514
Console:
        channel number: 0, channel name: console
Monitor:
        channel number: 1, channel name: monitor
```

```
SNMP Agent:
        channel number: 7, channel name: channel7
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 503, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 9, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 0
Logfile:
        channel number: 9, channel name: channel9, language: English
Information timestamp setting:
        log - date, trap - date, debug - date

 Sent messages = 15299, Received messages = 15299
```

也可以使用 **display channel** 命令查看 SNMP Agent 所用通道输出的信息。

```
<Router> display channel 7
channel number: 7, channel name: channel7
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL     ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging      N      debugging
c16a0000 IP       Y      debugging     Y      informational  N      debugging
```

还可使用 **display snmp-agent target-host** 命令查看 SNMP Agent 输出网管的信息。

```
<Router> display snmp-agent target-host
   Traphost list:
   Target host name: nms
   Traphost address: 10.1.1.1
   Traphost portnumber: 162
   Target host parameter: trapnms

   Total number is 1

   Parameter list trap target host:
   Parameter name of the target host: trapnms
   Message mode of the target host: SNMPV2C
   Trap version of the target host: v2c
   Security name of the target host: public

   Total number is 1
```

2.8　配置输出 Debug 信息

Debug 信息的输出可以配置指定模块的 Debug 信息输出到日志文件、控制台、终端和日志主机。但调试会占用设备的 CPU 资源，从而对系统的运行造成影响，因此，在调试之后要立即执行 undo debugging all 命令去使能调试。

2.8.1　Debug 信息输出配置任务

Debug 信息输出的配置任务总体上与 2.6 节介绍的 Log 信息输出的配置任务差不多，

也可分为基本功能和参数配置与输出配置两个方面。

1. Debug 信息输出基本功能和参数配置

Debug 信息输出基本功能和参数配置包括以下三个方面，分别与 **2.6.2 小节表 2-23 中第 2、3、5 步的对应配置方法基本一样**，只是要在第 5 步配置时间戳格式的命令中把“**log**”关键字替换成“debugging”，且二选一选项 millisecond 换成 second，**精确到秒**（**整条命令为 info-center timestamp debugging { { date | short-date | format-date } [precision-time { tenth-second | second }] | boot |none }**）。

① 使能信息中心。

②（可选）命名信息通道。

③（可选）配置 Debug 信息的时间戳。

2. Debug 信息输出配置

Debug 信息可选的输出方式与 2.6 节介绍的 Log 信息输出方式相比，仅少了一个不能输出到缓冲区，其他几种方式都支持。它们在配置上的区别与联系如下。

（1）配置 Debug 信息输出到日志文件

本项配置任务与 2.6.4 小节表 2-25 介绍的 Log 信息输出到日志文件的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **trap**，另外，在缺省情况下，系统向 9 号通道输出 Debug 信息的状态为 **off**，最低信息级别为 **debugging**（缺省情况下，系统向 9 号通道输出 Log、Trap 信息的状态为 **on**，最低信息级别为 **debugging**)，**且**这里配置的是 Debug 信息输出到日志文件。

（2）配置 Debug 信息输出到控制台或终端

这两项配置任务的配置方法与 2.6.5 小节表 2-26 介绍的 Log 信息输出控制台和输出到终端的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **debug**；另外，在缺省情况下，系统向 0 号（控制台）或 1 号（终端）通道输出 Trap 信息的状态为 **on**，最低信息级别为 **debugging**（Log 信息的最低信息级别为 **warning**)，且这里配置的是 Debug 信息输出到控制台或终端。

（3）配置 Debug 信息输出到日志主机

本项配置任务与 2.6.6 小节表 2-27 介绍的 Log 信息输出到日志主机的配置方法基本一样，仅需要将表中对应命令中 **log** 关键字替换为 **debug**；另外，在缺省情况下，系统向 2 号通道输出 Debug 信息的状态为 **off**，最低信息级别为 **debugging**（缺省情况下，系统向 2 号通道输出 Log 信息的状态为 **on**，最低信息级别为 **informational**)。

说明 配置好以上 Debug 信息输出后，可以使用 2.6.7 小节介绍的 **display info-center**、**display info-center statistics**、**display channel** [*channel-number* | *channel-name*]、**display info-center filter-id** [*id* | **bymodule-alias** *modname alias*]、**display info-center logfile path**、**display logfile** *file-name* [*offset* | **hex**] *命令进行 Debug 信息输出管理。

2.8.2 向控制台输出 Debug 信息的配置示例

本示例的基本拓扑结构如图 2-11 所示，PC 与 Router 通过 Console 口相连。用户希望在 PC 终端上查看 ARP 模块的调试信息。

1. 基本配置思路分析

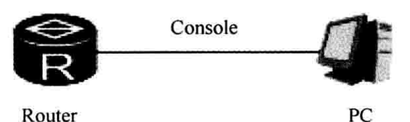


图2-11 向控制台输出Debug信息配置示例拓扑结构

根据2.8.1小节的介绍，并参考相关的2.6.5小节介绍的实际配置方法可以得出本示例的基本配置思路如下。

① 使能信息中心功能。

② 配置向控制台输出Debug信息的信息通道和输出规则，以实现Router产生的Debug信息发往控制台方向。

③ 使能终端显示功能，以实现用户能够在终端看到Router产生的Debug信息。

④ 打开ARP调试开关，使Router能产生ARP模块的Debug信息。

2. 具体配置步骤

① 使能信息中心功能。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] info-center enable
```

② 配置向控制台发送Debug信息的信息通道和输出规则，使用缺省的**console**信息通道（也即0号通道）向控制台发送ARP模块中**debugging**级别debug信息。

```
[Router] info-center source arp channel console debug level debugging state on
[Router] quit
```

③ 使能终端显示功能。

```
<Router> terminal monitor
Info: Current terminal monitor is on.
<Router> terminal debugging
Info: Current terminal debugging is on.
```

④ 打开ARP模块的调试开关。

```
<Router> debugging arp packet
```

配置好后，可通过 **display channel console** 命令查看配置的控制台通道信息，验证配置结果。

```
<Router> display channel console
channel number: 0, channel name: console
MODU_ID   NAME      ENABLE LOG_LEVEL      ENABLE TRAP_LEVEL      ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning        Y      debugging       Y      debugging
c16e0000 ARP      Y      warning        Y      debugging       Y      debugging
```

2.9 U盘开局配置与管理

U盘开局是指设备在开始部署时，用户预先将开局文件存储在U盘中，然后将U盘插入设备，让设备通过从U盘下载开局文件来完成自动升级及配置。U盘开局功能可大大简化开局部署流程，降低开局部署成本。**S系列交换机和AR G3系列路由器都支持U盘开局功能**。

2.9.1 U盘开局流程

U盘开局之前，需要先制作U盘开局索引文件（**要先关闭U盘写保护功能，且文件系统格式为FAT32**）；然后把U盘开局索引文件保存至U盘根目录下，把需要加载的开

局文件保存至U盘开局索引文件指定的目录下；最后将U盘插入设备中，设备会根据开局文件自动完成软件升级。整个U盘开局流程如图2-12所示，U盘插入设备后的运行流程如图2-13所示，具体说明如下。

① U盘插入需要开局的设备。

② 系统检测到U盘在位，检测U盘中是否存在U盘开局索引文件：如果存在，进入下一步；否则，不进行U盘开局，结束流程。

③ 检测U盘开局索引文件合法性：如果合法，进入下一步；否则，开局失败，结束流程。

④ 按照索引文件中的描述信息从U盘中获取开局文件，并将其保存至指定的存储介质中：如果获取文件成功，进入下一步；否则，开局失败，结束流程。

⑤ 将开局文件中所包括的文件（如系统软件、配置文件、补丁包文件、License文件等）设置为下次启动文件。

⑥ 设备重启。

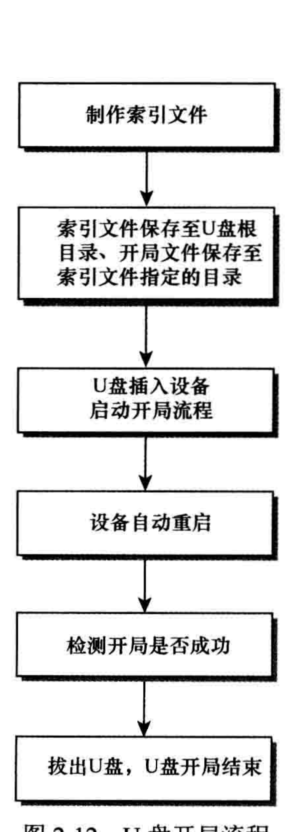


图2-12 U盘开局流程

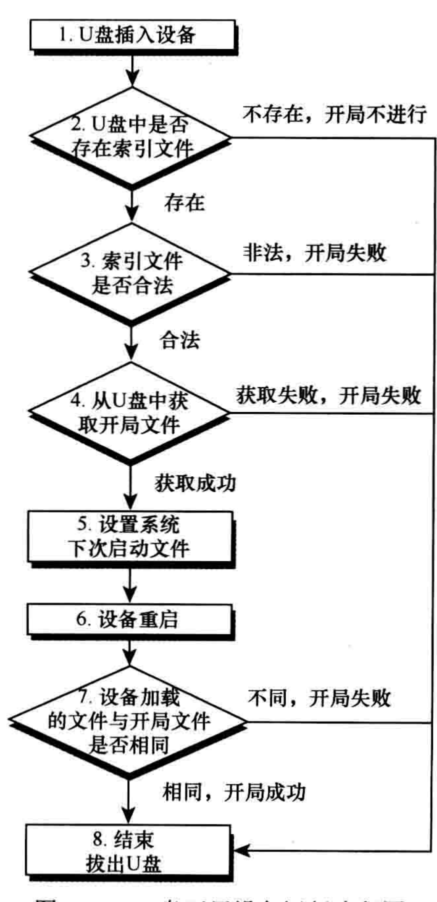


图2-13 U盘开局设备运行流程图

⑦ 设备重新启动后，系统检测当前设备加载的文件与开局文件是否相同，以判断开局状态，如果相同，开局成功；否则，开局失败，结束流程。

⑧ U盘开局流程结束。将U盘从设备中拔出。

2.9.2 U盘开局文件

AR G3系列路由器支持加载的开局文件包括必选文件和可选文件两类。必选文件为索引文件，名称必须为USB_AR.ini或usb_ar.ini；可选文件包括以下几种。

① 系统软件：后缀名为.cc。

② 配置文件：后缀名为.cfg或.zip。

③ 补丁文件：后缀名为.pat。

④ License文件：后缀名为.dat。

⑤ 语音文件：后缀名为.res。

⑥ 用户自定义文件。

S系列交换机支持加载的开局文件包括必选文件和可选文件两类。必选文件为索引文件，名称必须为usbload_config.txt；可选文件包括以下几种。

① 系统软件：后缀名为.cc。

② 配置文件：后缀名为.cfg或.zip。

③ 补丁文件：后缀名为.pat。

④ Web文件：后缀名为.web.zip或者.web.7z。

2.9.3 U盘开局索引文件制作

从上节介绍的U盘开局文件所包括的文件可以看出，必选的文件只有索引文件，所以制作索引文件是U盘开局的前提。U盘开局前，要保证开局设备可以正常启动，并且保证设备Flash或SD卡中有足够的存储空间来保存开局文件。

1. *U盘开局索引文件制作方法*

U盘开局索引文件的制作方法如下。

① 在PC上利用记事本之类的文本编辑软件新建一个空的文本文档。

② 按照下面即将介绍的U盘开局索引文件格式编辑文件内容。

③ 将此文本文档另存为USB_AR.ini或usb_ar.ini（在此仅以AR G3系列路由器的U盘开局索引文件制作为例进行介绍）。

④ 将USB_AR.ini或usb_ar.ini文件复制至U盘的根目录下。

2. *U盘开局索引文件格式*

U盘开局索引文件的格式如下（带"="的字段为需要具体配置的字段，带"[ ]"的字段为配置信息分类字段），其中各字段的说明如表2-29所示。

```
BEGIN AR
[USB CONFIG]
SN=
EMS_ONLINE_STATE=
[UPGRADE INFO]
OPTION=
AUTOFLAG=
PASSWORD=
DEVICENUM=
[DEVICEn DESCRIPTION]
OPTION=
```

```
ESN=
MAC=
VERSION=
DIRECTORY=
FILENUM=
TYPEn=
FILENAMEn=
END AR
```

表 2-29 索引文件字段含义

字段	描述
BEGIN AR	起始标志，不能修改
USB CONFIG	U 盘配置信息，表示下面为配置信息，不能修改
SN	数据变更时间标识，也即执行新的 U 盘开局时间，其格式为：年月日.时分秒。例如，2013 年 10 月 30 日 10 时 10 分 10 秒，则设置为 SN=20131030.101010 【说明】SN 字段是 U 盘开局的一个标识。设备有一个默认的 U 盘开局标识，当 U 盘上有新的.ini 文件时，就会对比设备原有的 U 盘开局 SN 号和新的.ini 文件中 SN 号是否一致。如果不一致，则触发 U 盘开局，使用 U 盘指定的开局文件启动。开局成功后，设备的开局 SN 号会更新为.ini 文件中设置的 SN 号
EMS_ONLINE_STATE	网管在线标识，YES 代表网管在线，NO 代表网管不在线。如果设置为 YES 时，则在开局时有些流程可能会要求网管进行交互确认，如果设置为 NO，则不会提示网管进行交互确认。通常为不在线，让系统自动升级
UPGRADE INFO	升级信息头，表示下面为信息头设置内容，不能修改
OPTION	升级模式标识，固定为 OPTION=AUTO
AUTOFLAG	密码认证标识，0 代表不认证，当 U 盘开局不需要安全认证时选择；1 代表认证，当 U 盘开局需要安全认证时选择。选择认证方式，在 U 盘插入设备时，系统会比较此索引文件指定的密码与设备配置的密码是否一致，如果一致，启动开局；否则，开局失败 该字段是可选配置信息，缺省为不认证
PASSWORD	指定 U 盘开局安全认证的密码。该字段也是可选信息，仅当前面的 AUTOFLAG 字段为 1 时才需要输入，且该密码必须与通过 **set usb autoupdate password** 命令配置的密码保持一致
DEVICENUM	指定用此索引文件进行升级的设备数。 ● 如果仅需要给一台设备升级软件版本，则设置 DEVICENUM=1，下面的 ESN 字段的取值为设备序列号，MAC 字段的取值为设备的 MAC 地址 ● 如果需要给多台同系列的设备升级至同一版本，则设置 DEVICENUM=1，下面的 ESN 和 MAC 字段的取值都仅可为 DEFAULT ● 如果需要给多台设备升级至不同版本，DEVICENUM 的取值为需要升级设备的数目，ESN 和 MAC 字段的取值根据设备的实际情况填写
DEVICE*n* DESCRIPTION	设备 *n* 的描述信息头，*n* 的取值为整数类型，取值范围：1～100 设备的描述信息包括升级标识、设备序列号、设备 MAC 地址、升级版本号、开局文件的存储路径、需要加载的文件个数、标识升级的文件类型和升级的文件名
OPTION	指定用于标识当前设备是否需要升级，OK 表示需要升级；NOK 表示不需要升级
ESN	指定要升级的设备的序列号。如果 ESN=DEFAULT 或者为空，则表示 U 盘索引文件匹配所有设备。否则，表示匹配某一台设备的序列号

（续表）

字段	描述
MAC	指定要升级的设备的 MAC 地址。如果 MAC=DEFAULT 或者为空，则表示 U 盘索引文件匹配所有设备。否则，表示匹配某一台设备的 MAC 地址
VERSION	升级版本号，要与需要升级的系统软件版本一致。但该字段内容可以为空
DIRECTORY	指定用于标识开局文件的存储路径： • 若 DIRECTORY=DEFAULT 或者为空，则文件位于 U 盘根目录下 • 若 DIRECTORY=/abc，则文件位于 U 盘的 abc 文件夹下
FILENUM	指定需要加载的文件个数。例如设备仅需要加载系统软件，那么 FILENUM 的取值为 1；如果设备需要同时加载系统软件和补丁文件，那么 FILENUM 的取值为 2
TYPE*n*	指定用于标识升级的文件类型（*n* 的取值从 1 开始，每个文件分配一个序号）： • SYSTEM-SOFTWARE：系统软件 • SYSTEM-CONFIG：配置文件 【说明】如果设备支持语音功能且工作在 PBX 模式时，配置文件表示为 SYSTEM-CONFIG_PBX；如果设备支持语音功能且工作在 SIPAG 模式时，配置文件表示为 SYSTEM-CONFIG_SIPAG SYSTEM-PAT：补丁文件；SYSTEM-LICENSE：License 文件；SYSTEM-VOICE：语音文件；USER-DEFINE：用户自定义文件
FILENAME*n*	指定用于标识升级的文件名（*n* 的取值从 1 开始，每个文件分配一个序号）。例如 TYPE1=SYSTEM-SOFTWARE，U 盘相应目录中系统软件的名称为 system-software.cc，则 FILENAME1=system-software.cc
END AR	文件结束标志

说明　可从设备表面贴的标签上查看设备的系统 MAC 地址和 ESN 序列号，也可登录到设备上分别执行 **display system-mac** 和 **display esn** 命令查看设备的系统 MAC 地址和 ESN 序列号。

3. U 盘开局索引文件示例

【示例 1】制作用于升级一台设备的索引文件，需求如下。

- 数据变更时间为 2013 年 10 月 28 日 10 时 10 分 10 秒。
- 网管不在线。
- 需要进行升级。
- 进行密码认证。
- 设备 ESN 为 00080123456789，设备 MAC 为 0018-0303-1234。
- 系统软件位于 U 盘根目录下，名称为 system-software01.cc，版本号为 V200R001C00SPC200。
- 其他字段均采用缺省值。

则对应的索引文件如下。

```
BEGIN AR
[USB CONFIG]
SN=20131028.101010
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
```

```
OPTION=AUTO
AUTOFLAG=1
PASSWORD=12345A
DEVICENUM=1
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=00080123456789
MAC=0018-0303-1234
VERSION=V200R001C00SPC200
DIRECTORY=DEFAULT
FILENUM=1
TYPE1=SYSTEM-SOFTWARE
FILENAME1=system-software01.cc
END AR
```

【示例 2】制作用于将多台设备升级至同一软件版本的索引文件，需求如下。

- 数据变更时间为 2013 年 10 月 28 日 10 时 10 分 10 秒。
- 网管不在线。
- 需要进行升级。
- 不进行密码认证。
- 系统软件和配置文件位于 U 盘根目录下，名称分别为 system-software01.cc 和 system-config02.zip，版本号为 V200R001C00SPC200。
- 其他字段均采用缺省值。

则对应的索引文件如下，这里要对两个开局文件分别配置 TYPE 和 FILENAME 字段值。

```
BEGIN AR
[USB CONFIG]
SN=20131028.101010
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
AUTOFLAG=0
DEVICENUM=1
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=DEFAULT
MAC=DEFAULT
VERSION=V200R001C00SPC200
DIRECTORY=DEFAULT
FILENUM=2
TYPE1=SYSTEM-SOFTWARE
FILENAME1=system-software01.cc
TYPE2=SYSTEM-CONFIG
FILENAME2=system-config02.zip
END AR
```

【示例 3】制作用于两台描述信息不一致的索引文件，需求如下。

- 数据变更时间为 2013 年 10 月 28 日 10 时 10 分 10 秒。
- 网管不在线。
- 不进行密码认证。
- 第一台设备的 ESN 为 00080123456789，MAC 为 0018-0303-1234，系统软件名称

为 arv200r002.cc，版本号为 V200R002，不需要加载配置文件。

- 第二台设备的 ESN 为 66680123456789，MAC 为 0018-0303-5678，系统软件名称为 arv200r003.cc，版本号为 V200R003，需要加载的配置文件为 arv200r003.zip。

则对应的索引文件如下，这里要对两台设备分别配置 OPTION 及以下的所有字段。

```
BEGIN AR
[USB CONFIG]
SN=20110628.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
AUTOFLAG=0
DEVICENUM=2
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=00080123456789
MAC=0018-0303-1234
VERSION=V200R002
DIRECTORY=DEFAULT
FILENUM=1
TYPE1=SYSTEM-SOFTWARE
FILENAME1=arv200r002.cc
[DEVICE2 DESCRIPTION]

OPTION=OK
ESN=66680123456789
MAC=0018-0303-5678
VERSION=V200R003
DIRECTORY=DEFAULT
FILENUM=2
TYPE1=SYSTEM-SOFTWARE
FILENAME1=arv200r003.cc
TYPE2=SYSTEM-CONFIG
FILENAME2=arv200r003.zip
END AR
```

2.9.4　配置 U 盘开局认证

U 盘开局之前，首先要按照上节介绍的方法制作 U 盘开局索引文件，然后把 U 盘开局索引文件保存至 U 盘根目录下，把需要加载的开局文件保存至 U 盘开局索引文件 DIRECTORY 字段设置的目录下，最后将 U 盘插入设备中启动 U 盘开局流程。

U 盘开局时需要注意以下几点。

① U 盘规格：文件系统格式是 FAT32，硬件接口是标准的 USB 2.0。

② U 盘开局支持经华为认证的指定型号的 U 盘，以保证 U 盘和设备的良好兼容性。

③ 使用 U 盘进行写操作时，请务必保证关闭 U 盘写保护功能。

④ U 盘开局前，保证开局设备可以正常启动，并且保证设备 Flash 或 SD 卡中有足够的内存空间用来保存开局文件。

⑤ U 盘开局不支持同时插入两个 U 盘进行开局。

⑥ U 盘开局文件包括：U 盘开局索引文件，系统软件、配置文件、补丁文件、语音文件和 License 文件。其中，U 盘开局索引文件是必选的，其他几个开局文件至少选择

一个。

⑦ 升级时文件复制过程中设备不能断电，否则会造成升级失败甚至会造成设备无法启动。

⑧ 升级结束之前不能将 U 盘拔出，否则可能会造成 U 盘内的数据损坏。

在 U 盘开局配置中可能需要配置开局认证密码，可以在用户视图下通过 **set usb autoupdate password** *password* 命令进行配置。参数 *password* 用来指定 U 盘开局的认证密码，1～64 个字符，区分大小写，不支持空格。

说明 当用户需要 U 盘开局密码认证功能时，可通过此命令配置 U 盘开局的认证密码。此时，U 盘开局索引文件的“AUTOFLAG”字段必须为 1，并且“PASSWORD”字段的内容要与此命令配置的 U 盘开局认证密码保持一致。

当用户需要取消 U 盘开局密码认证功能时，可在用户视图下通过 **clear usb autoupdate password** 命令删除前面通过 **set usb autoupdate password** 命令配置的 U 盘开局认证密码。此时，U 盘开局索引文件的“AUTOFLAG”字段必须为 0 或空或不存在。

全部准备好后，可将保存开局文件的 U 盘插入设备 USB 接口上，启动开局流程。进入开局流程后，系统首先按照 USB_AR.ini 文件中的描述信息从 U 盘中获取开局文件复制到设备缺省的存储介质中。然后设备将系统软件、配置文件设置为系统下次启动文件。最后，设备自动重启。确认 U 盘开局成功后，拔出 U 盘，U 盘开局结束。

可通过执行 **display usb** *usb-id* **autoupdate state** 命令查看 U 盘开局的进行状态。也可通过 ACT 指示灯的状态，判断 U 盘开局进行的状态。

① 绿灯常亮：U 盘开局成功。

② 绿灯闪烁：U 盘开局正在进行中。

③ 红灯常亮：U 盘开局失败。

2.10 Auto-Config 配置与管理

Auto-Config（自动配置）是指**新出厂或空配置设备**加电启动时采用的一种自动加载版本文件（包括系统软件、补丁文件或配置文件）的功能。

在部署网络设备时，设备安装完成后，需要软调工程师到安装现场，对设备进行软件调试。当设备数量较多、分布较广时，维护人员需要在每一台设备上进行手工配置，这样既影响了设备部署的效率，又大大增加了人力成本。设备运行 Auto-Config 功能，可以从文件服务器获取版本文件并自动加载版本文件，实现远程部署接入网络的设备，从而减少人力成本，并提高了设备部署的效率，解决了设备数量多、手工配置人力成本高的问题。**华为 S 系列交换机和 AR G3 系列路由器均支持 Auto-Config 功能。**

2.10.1 Auto-Config 工作原理

Auto-Config 功能的基本工作原理是利用 DHCP 服务器功能为担当 DHCP 客户端的配置设备自动分配基础配置信息，利用存放了 Auto-Config 配置文件的 FTP 或者 TFTP

服务器自动为待配置设备加载版本文件（包括配置文件、系统软件、补丁文件和 Web 文件）。

如图 2-14 所示，RouterA、RouterB、RouterC 和 RouterD 运行 Auto-Config 功能后，设备作为 DHCP 客户端定时向 DHCP 服务器发送 DHCP 请求报文以获得配置信息，然后 DHCP 服务器向待配置设备响应 DHCP 应答报文，报文内容包括分配给待配置设备的 IP 地址、文件服务器的 IP 地址、文件服务器的登录方式、版本文件的配置信息，最后设备根据收到的 DHCP 响应报文中携带的配置信息向指定的文件服务器自动获取版本文件，并设置为下次启动加载的文件，待设备自动重启后就实现了版本文件的自动加载。

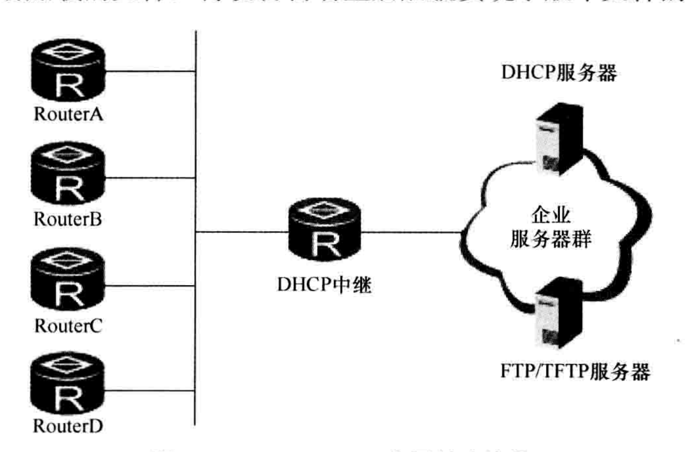


图 2-14　Auto-Config 应用基本结构

在 Auto-Config 功能实现中，包括以下几种角色的设备。

① DHCP 服务器：Auto-Config 开始运行时，待配置设备作为 DHCP 客户端向 DHCP 服务器请求网络配置信息。DHCP 服务器上需要配置动态地址池（用来为待配置设备分配接口 IP 地址）、待配置设备的出口网关地址、Option 参数（包括 DHCP 服务器需要向 DHCP 客户端分配的文件服务器的 IP 地址、需要加载的版本文件名称等信息）。

② DHCP 中继：当待配置设备与 DHCP 服务器位于不同网段时，则还需要通过配置 DHCP 中继实现待配置设备与 DHCP 服务器之间的报文交互。

③ FTP/TFTP 文件服务器：文件服务器上存放着 Auto-Config 需要加载的版本文件（包括配置文件、系统软件、补丁文件和 Web 文件）。当 DHCP 服务器向待配置设备返回文件服务器的 IP 地址后，待配置设备就会向指定 IP 地址的文件服务器获取版本文件并设置为下次启动的版本文件。

④ 中间文件：当 DHCP 的 Option 信息没有 Option 67（配置文件的 Option 信息）时，Auto-Config 功能将通过中间文件解析出需要下载的版本文件信息。中间文件存放在 FTP/TFTP 文件服务器上，其内容为设备 MAC 地址或 ESN 序列号与系统软件名称、系统软件的版本号、补丁文件名称、Web 文件名称和配置文件名称的对应关系。

2.10.2　Auto-Config 特性的产品支持

AR G3 系列路由器和 S 系列交换机，根据设备与 DHCP 服务器是否在同一网段可采用不同的部署方式。下面分别予以介绍。

1. 同网段 Auto-Config 部署

当待配置设备与 DHCP 服务器位于同一网段时，可以通过图 2-15 所示的组网图部署 Auto-Config 功能。FTP/TFTP 服务器上存放必选的配置文件以及可选的系统软件、补丁文件和中间文件，且与待配置设备、DHCP 服务器路由可达。软件调测人员配置 DHCP 服务器及 FTP/TFTP 服务器后，待配置设备可以通过 Auto-Config 功能从 FTP/TFTP 服务器获取版本文件并自动加载相应的文件。

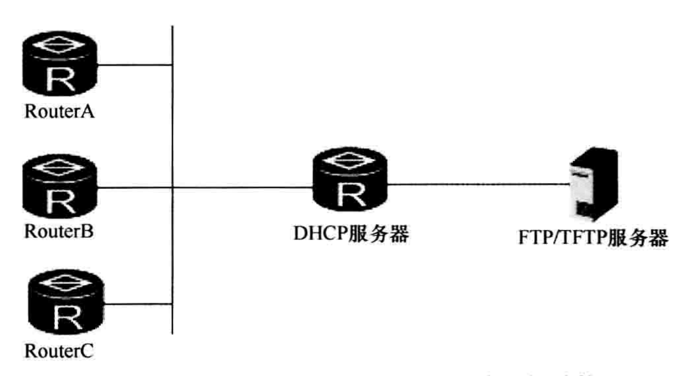


图 2-15　Auto-Config 同网段部署基本网络结构

这种部署方式适合网络规模较小，待配置设备分布相对集中的场景中。

2. 跨网段 Auto-Config 部署

当待配置设备与 DHCP 服务器位于不同网段时，可以通过图 2-16 所示的组网图部署 Auto-Config 功能。FTP/TFTP 服务器上存放必选的配置文件以及可选的系统软件、补丁文件和中间文件，且与待配置设备、DHCP 中继、DHCP 服务器路由可达。软件调测人员配置 DHCP 中继、DHCP 服务器及 FTP/TFTP 服务器后，待配置设备可以通过 Auto-Config 功能从 FTP/TFTP 服务器获取版本文件并完成自动加载相应的文件。

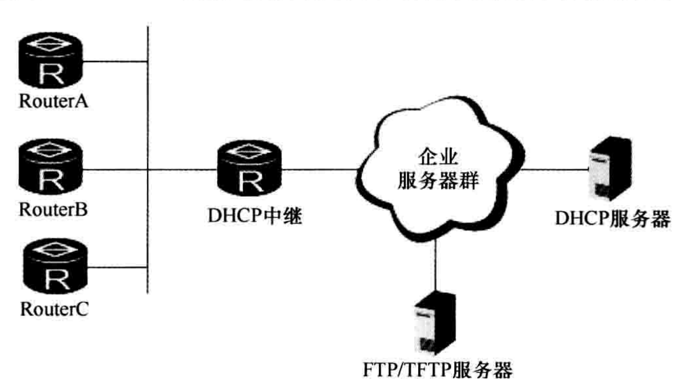


图 2-16　Auto-Config 跨网段部署的基本网络结构

这种部署方式适合网络规模较大，待配置设备分布相对分散的场景中，多个网段的待配置设备可以使用同一个 DHCP 服务器，既节省了成本，又便于集中管理。

但在配置 Auto-Config 功能前，需要注意以下事项。

① 在开局部署场景中，用户可选择使用 Auto-Config 功能或人工配置。若选择人工配置，Auto-Config 功能将自动关闭。

② Auto-Config 功能与 U 盘开局功能互斥，两者只能选其一。

③ 待配置设备必须为新出厂或空配置文件的设备，即设备中不能存在后缀名为.cfg 和.zip 的文件（*.web.zip 文件除外）。

④ 待配置设备的系统 MAC 地址和 ESN 序列号可以通过以下方式获取。

- 设备表面贴的标签上可以查看设备的系统 MAC 地址和 ESN 序列号。
- 如果可以登录到设备，可分别执行 **display system-mac** 诊断视图（在系统视图下执行 **diagnose** 命令进入）命令和 **display esn** 任意视图命令查看设备的系统 MAC 地址和 ESN 序列号。

⑤ AR G3 系列路由器中支持 Auto-Config 功能的接口情况如下。

- AR151：Eth0/0/4
- AR201：Eth0/0/8
- AR1200 系列、AR2200 系列、AR3200 系列：GE0/0/1
- AR1220：GPON 接口

⑥ 用户通过 Console 口登录新出厂（或空配置启动）的设备时，系统会提示："Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:"

如果需要运行 Auto-Config 功能，键入 n，并按 Enter 键；如果不需要运行 Auto-Config 功能，键入 y，并按 Enter 键。**注意：如果不需要运行 Auto-Config，但选择的是 n，会导致后续配置的 DHCP 服务器、路由、DNS 服务器和 VTY 用户配置丢失。**

2.10.3 配置同网段 Auto-Config 功能

当待配置设备和 DHCP 服务器在同一网段时，则可以通过配置同网段 Auto-Config 功能自动加载系统软件、补丁文件和配置文件，实现设备的远程部署。

在配置同网段 Auto-Config 功能之前，需确保 DHCP 服务器、文件服务器（FTP/TFTP 服务器）到待配置设备的路由可达，并确保待配置设备中没有启动配置文件（Startup-Config）。

配置同网段 Auto-Config 功能包括：使能 Auto-Config 功能、（可选）编辑中间文件、配置 DHCP 服务器和 FTP/TFTP 文件服务器（这些任务根据组网环境需要分别在不同的设备上进行配置，且各任务之间为并列关系）。上述任务配置完毕后，再对设备上电启动 Auto-Config 流程。

1．使能 Auto-Config 功能

此配置任务是在待配置设备上进行配置的。可以先在用户视图下执行 **display autoconfig enable** 命令查看待配置设备当前的 Auto-Config 功能运行状态，如果处于去使能状态，则可在系统视图下执行 **autoconfig enable** 命令使能 Auto-Config 功能。

Auto-Config 功能缺省情况下处于使能状态。因此，如果是新出厂的设备配置 Auto-Config 功能，不需要执行此任务。当自动配置完成后，需在系统视图下执行 **undo autoconfig enable** 命令去使能 Auto-Config 功能，此时通过 **display autoconfig-status** 命令查看时会发现 Auto-Config 功能处于 stop 状态。如果你已通过 Console 口登录设备，

执行 **undo autoconfig enable** 命令，看到“Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:”提示后输入 y，确认去使能操作即可。

注意 在 Auto-Config 功能运行过程中出现问题需要人工处理时，Auto-Config 功能不能自动恢复，如果要继续进行 Auto-Config 功能，也需先执行 **undo autoconfig enable** 系统视图命令去使能 Auto-Config 功能，然后通过执行 **autoconfig enable** 系统视图命令重新使能 Auto-Config 功能。

2.（可选）编辑中间文件

在 Auto-Config 功能中需要获取用于在待配置设备上加载的配置文件。这有两种方式，优先通过 DHCP 服务的 Option 67 参数来获取配置文件；如果配置 DHCP 服务器时没有配置 Option 67 参数，则可以通过中间文件来完成配置文件以及可选的系统软件、补丁文件的自动加载。

通过在 DHCP 服务器上配置 Option 67 参数获取配置文件的方式适用于待配置设备较少，不同设备加载相同配置文件的场景；而通过文件服务器上的中间文件获取配置文件的方式适用于待配置设备较多，不同设备加载不同配置文件的场景。此处仅介绍“中间文件”方式。

中间文件是通过文本编辑软件，根据设备的系统 MAC 地址或 ESN 与所需的系统软件、补丁文件和配置文件名称进行编辑的，存放在 FTP/TFTP 服务器上，其内容为设备系统 MAC 地址或 ESN 序列号与系统软件名称、系统软件的版本号、补丁文件名称和配置文件名称的对应关系。当设备获得 FTP/TFTP 服务器的 IP 地址后，就从 FTP/TFTP 服务器下载中间文件进行解析，查询到与本设备 MAC 地址或 ESN 序列号匹配的系统软件名称、系统软件的版本号、补丁文件名称和配置文件名称，然后根据名称从 FTP/TFTP 服务器下载文件。

编辑中间文件的具体步骤如下。

① 在文本编辑软件中新建一个文本文档，文件命名为 arnet.ini。

② 中间文件包括 5 个字段：MAC（设备 MAC 地址）或 ESN、vrpfile（VRP 系统软件版本文件）、vrpver（VRP 系统软件版本号）、patchfile（补丁文件）和 cfgfile（配置文件）。其中配置文件为必选，其他均为可选。其格式如下。

```
MAC= ;vrpfile= ;vrpver= ;patchfile= ;cfgfile= ;
```

或

```
ESN= ;vrpfile= ;vrpver= ;patchfile= ;cfgfile= ;
```

下面通过一个具体的示例进行介绍。假设一台待配置设备的 MAC 地址为 0018-82C5-AA89，设备序列号 ESN 为 9300070123456789，对应这台设备应下载的版本文件名为 auto_V200R003C01.cc，版本号信息为 V200R003C01，补丁文件为 auto_V200R003C01.pat，配置文件为 auto_V200R003C01.cfg，则中间文件 arnet.ini 内容如下**（要用一行输入，不能手动分行，分号为英文分号，且最后的分号也不能少）**。

```
MAC=0018-82C5-AA89;vrpfile=auto_V200R003C01.cc;vrpver=V200R003C01;patchfile=auto_V200R003C01.pat;cfgfile=
auto_V200R003C01.cfg;
```

或

```
ESN=9300070123456789;vrpfile=auto_V200R003C01.cc;vrpver=V200R003C01;patchfile=auto_V200R003C01.pat;cfgfile
=auto_V200R003C01.cfg;
```

说明　当有多台设备需要配置时，中间文件的每行对应一台设备的配置信息。最多支持 1 000 台设备通过中间文件实现 Auto-Config 功能。

中间文件的配置项中，**系统 MAC 地址和设备序列号 ESN 必选其一；配置文件为必选项，**系统软件和补丁文件为可选项，三者间没有顺序限制。

中间文件中系统软件名和版本号信息必须同时存在，并且系统软件名中的版本号信息与中间文件中的版本号信息一致。版本号 vrpver 信息必须全部包含在系统软件 vrpfile 信息中。

3. 配置 DHCP 服务器

需要运行 Auto-Config 的设备在加电之前，需先部署 DHCP 服务器和文件服务器，保证设备能正常获取 IP 地址、网关、DNS 服务器以及配置文件的信息。要求 DHCP 服务器必须支持配置相关的 DHCP 服务器 Option 参数选项。有关 DHCP 服务器地址池的配置方法参见本书第 5 章，可以配置基于全局地址池的 DHCP 服务器或基于接口地址池的 DHCP 服务器。

在配置 IP 地址池时，所配置的 IP 地址范围应该避免使用需要加载的配置文件里面已经配置的 IP 地址（可排除配置文件里面已经配置的 IP 地址），以防止地址冲突。要特别注意的是，可执行 **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* <1-8> }命令来配置 DHCP 服务器的 Option 参数选项。可选的 DHCP 选项如表 2-30 所示。

表 2-30　Auto-Config 特性中使用到 DHCP Option

Option 编号	描述
Option 43	表示自动配置服务器 ACS（接入控制服务器）的配置信息如下 ● sub-option 1：ACS URL 信息。格式为：URL=URL_INFO。例如：URL=http://192.168.1.40:80/acs; ● sub-option 2：ACS 用户名密码信息。格式为：username=USERNAME; password=PASSWORD; 路由器设备不支持做 ACS 服务器
Option 67	表示为 DHCP 客户端分配的配置文件名称。**这是用来指派配置文件的 DHCP 选项**
Option 141	表示为 DHCP 客户端分配的 FTP 用户名
Option 142	表示为 DHCP 客户端分配的 FTP 用户密码
Option 143	表示为 DHCP 客户端分配的 FTP 服务器 IP 地址
Option 145	表示为 DHCP 客户端分配的非配置文件信息。例如：系统软件信息、版本号信息和补丁文件信息（版本号 vrpver 信息必须全部包含在系统软件 vrpfile 信息中） 格式为：vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME 例如：vrpfile=auto_V200R003C01.cc; vrpver=V200R003C01; patchfile=auto_V200R003C01.pat;
Option 146	表示用户指定动作的操作信息，包括空间不足时删除文件的策略和配置文件延迟生效时间，格式如下 ● opervalue=0：表示空间不足时，不删除文件系统中系统软件。opervalue=1：表示空间不足时，删除文件系统中系统软件。缺省情况下，opervalue=0

（续表）

Option 编号	描述
Option 146	• delaytime：表示 Auto-Config 下载配置文件成功后，配置的延时重启生效时间，单位为秒。缺省情况下，delaytime=0，延时重启生效时间最大为一天，即 86 400 s。如果配置的时间大于一天，则按一天计算
Option 147	表示认证信息。可以不配置，如果配置，必须配置为 AutoConfig
Option 150	表示为 DHCP 客户端分配的 TFTP 服务器 IP 地址

说明 配置 Option 150，直接获取 TFTP 服务器的 IP 地址；配置 Option 141、142、143，获取 FTP 用户名、FTP 密码、FTP 服务器的 IP 地址。待配置设备获取的文件服务器账号仅用于 Auto-Config 开局部署场景，待配置设备不会保存文件服务器的用户名和密码。

如果没有配置 Option 67 参数，Auto-Config 功能需要通过前面介绍的中间文件实现配置文件的自动加载。Auto-Config 功能部署完成后，要删除 DHCP 服务器的相关配置，避免对 DHCP 服务器上其他配置信息造成影响。

4. 配置文件服务器

当文件服务器为 FTP 服务器时，IP 地址需要和 DHCP 服务器上配置的 Option 143 保持一致；当文件服务器为 TFTP 服务器时，IP 地址需要和 DHCP 服务器上配置的 Option 150 保持一致。

文件服务器建议采用 FTP 方式。文件服务器可以是路由器，也可以是 PC。在交换机或路由器上配置 FTP 文件服务器的方法，可参见配套图书《华为交换机学习指南》第 3 章 3.7.2 小节。

配置完文件服务器后，将中间文件（可选）、系统软件（可选）、补丁文件（可选）和配置文件（必选）放至文件服务器的工作目录（在配置 FTP 服务器时指定）下。

如果 PC 作为文件服务器，将文件直接复制到 PC 的工作目录（文件服务器软件需要设置工作目录）下；如果用交换机或路由器作为文件服务器，可通过文件客户端应用程序将文件上传到文件服务器的工作目录下。

为充分保证文件服务器的安全，建议配置的文件服务器用户名唯一，并将其权限设置为只读，防止进行非法修改；Auto-Config 过程结束后，请关闭相应的文件服务器功能。

5. 设备上电启动 Auto-Config 流程

上述配置步骤完成后，将待配置 Auto-Config 设备上电启动（或重新启动），Auto-Config 功能会自动运行。

可通过执行 **display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* }**used** 任意视图命令查看 DHCP 服务器为待配置设备分配的 IP 地址信息；执行 **display autoconfig-status** 命令查看 Auto-Config 功能的运行状态；执行 **display startup** 命令查看设备本次及下次启动加载的系统软件和配置文件。

2.10.4 配置跨网段 Auto-Config 功能

当待配置 Auto-Config 功能的设备和 DHCP 服务器在不同网段时，可以通过配置跨网段 Auto-Config 功能自动加载系统软件、补丁文件和配置文件，实现设备的远程部署。

在配置跨网段 Auto-Config 功能之前，需确保 DHCP 服务器、DHCP 中继、文件服务器（FTP/TFTP 服务器）到待配置设备的路由可达；确保待配置设备中没有配置启动配置文件。

配置跨网段 Auto-Config 功能所包括的配置任务有使能 Auto-Config 功能、编辑中间文件、配置 DHCP 服务器、配置 DHCP 中继和配置 FTP/TFTP 文件服务器（需根据组网环境分别在不同的设备上进行配置，且各任务之间为并列关系）。上述任务配置完毕后，再对设备上电启动 Auto-Config 流程。

从以上配置任务可以看出，跨网段的 Auto-Config 功能配置与上节介绍的同网段的 Auto-Config 功能配置主要不同就是多了一个用于在 DHCP 客户端（待配置设备）和 DHCP 服务器间转发 DHCP 服务报文的 DHCP 中继代理设备的配置，其他配置基本一样。

1. 使能 Auto-Config 功能

本项配置任务的具体配置方法参见上节第 1 小点介绍的“使能 Auto-Config 功能”的方法。

2. （可选）编辑中间文件

本项配置任务的具体配置方法参见上节第 2 小点介绍的“编辑中间文件”的方法。**仅当没有在 DHCP 服务器中配置 Option 67 时才需要配置。**

3. 配置 DHCP 服务器

本项配置任务的具体配置方法参见上节第 3 小点介绍的“配置 DHCP 服务器”的方法。

4. 配置 DHCP 中继

当待配置设备与 DHCP 服务器不在同一网段时，需要配置 DHCP 中继实现待配置设备从 DHCP 服务器的全局地址池中获取 IP 地址等配置信息。DHCP 客户端与 DHCP 服务器之间可以有多个 DHCP 中继设备，且最多支持 16 个。

有关 DHCP 中继的配置方法请参见本书第 5 章，但 Auto-Config 功能部署完成后，要删除 DHCP 中继的相关配置，以保证 DHCP 中继的安全。

5. 配置文件服务器

本项配置任务的具体配置方法参见上节第 4 小点介绍的“配置文件服务器”的方法。

6. 设备上电启动 Auto-Config 流程

上述配置步骤完成后，将待配置 Auto-Config 设备上电启动（或重新启动），Auto-Config 功能会自动运行。

除了可以用到上节介绍的 display 命令查看 Auto-Config 功能相关信息外，还可以通过执行 **display dhcp relay** { **all** | **interface** *interface-type interface-number* }命令查看接口对应的 DHCP 服务器或服务器组的信息；通过执行 **display dhcp server group** [*group-name*]命令查看 DHCP 中继设备的 DHCP 服务器组的配置信息。

2.10.5 Auto-Config 维护

通过监控设备 Auto-Config 各个阶段运行的状态，保证 Auto-Config 功能的正常运行。

① 待配置设备上电启动 5 min 后，用户可以执行 **display ip pool** {interface *interface-pool-name* | **name** *ip-pool-name* } **used** 命令可以查看 DHCP 服务器为待配置设备分配 IP

地址信息，验证待配置设备是否已成功接入链路。

② 待配置设备成功获取 IP 地址后 5 min，用户可以查看文件服务器的文件传送日志，或登录到待配置设备执行 **display autoconfig-status** 命令查看是否已经下载正确的系统软件、补丁文件和配置文件及 Auto-Config 运行情况。**但不要在待配置设备上做 Save 操作**，因为当前配置还未生效，如果 Save，保存的是临时文件。

如果由于获取文件失败导致流程处于挂起状态，可以通过执行 **autoconfig getting-file restart** 系统视图命令重新获取系统软件、补丁文件和配置文件，继续 Auto-Config 流程。

③ 待配置路由器正确下载文件后，根据用户的配置（Option 146）延时重启生效。可以通过执行 **display autoconfig activating-config delay** 命令查看配置的延时重启生效时间；可以通过执行 **display autoconfig activating-config remanent-time** 命令查看配置的延时重启生效的剩余时间。

2.10.6 同网段 Auto-Config 功能的配置示例

本示例的基本拓扑结构如图 2-17 所示，在小区接入组网环境下的开局部署场景中，汇聚设备 RouterD 连接着整个小区各个楼层的新出厂设备（如 RouterA、RouterB 和 RouterC）。用户希望为小区内的各楼层的新设备加载相同的系统软件、补丁文件和配置文件；并且由于待配置的新设备较多，为了降低人工成本、节省开局部署的时间，用户希望各楼层设备能实现统一自动的配置。

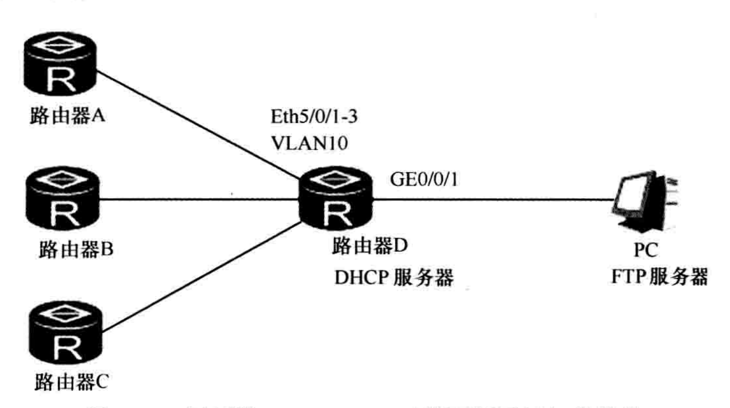


图 2-17 同网段 Auto-Config 功能配置示例拓扑结构

1. 基本配置思路分析

按照 2.10.3 小节介绍的配置任务及它们的配置方法，可以得出本示例的基本配置思路如下。

① 用一台与 RouterD 直接相连的 PC 担当 FTP 服务器。将需要加载的配置文件、系统软件和补丁文件放至 FTP 服务器的工作目录下。

② 在 RouterD 上配置 DHCP 服务器，为 RouterA、RouterB 和 RouterC 提供网络配置信息。由于待配置设备需加载相同的系统软件、补丁文件和配置文件，所以在配置 DHCP 服务器时，通过 Option67 和 Option145 提供需加载文件的信息。

③ 对 RouterA、RouterB 和 RouterC 上电，实现通过 Auto-Config 功能自动加载配置文件、系统软件和补丁文件。缺省情况下，设备的 Auto-Config 功能处于使能状态。

2. 具体配置步骤

① 配置 FTP 服务器的 IP 地址、用户名、密码及工作目录。

在 PC 上运行 FTP Server 程序（现仅以 wftpd32 软件为例进行介绍），在 wftpd32 软件主界面中依次选择“Security”→“Uers/rights”菜单项，打开如图 2-18 所示的对话框。然后单击“New User…”按钮，在打开的对话框中设置用户名为 **user** 和密码 **huawei**。然后在“Home Directory:”文本框中设置 PC 上 FTP 的工作目录为 D:\autoconfig。然后单击“Done”按钮完成设置并关闭对话框。配置 PC 的 IP 地址假设为 192.168.1.6，掩码为 255.255.255.0。

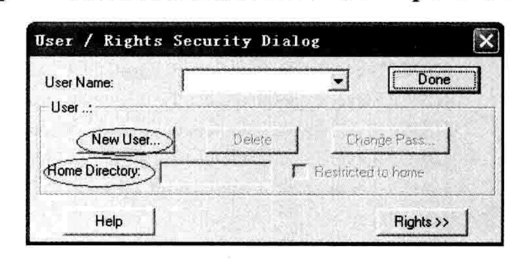


图 2-18 wftpd32 用户配置对话框

② 将用于分配给待配置设备的配置文件、系统软件和补丁文件上传至 FTP 服务器的工作目录 D:\autoconfig 上（从保存这些文件的设备上通过 FTP 协议上传，或者其他 PC 中复制）

③ 配置 DHCP 服务器。首先按照图示配置各接口加入 VLAN 10，并配置 GE0/0/1 接口和 VLANIF10 接口的 IP 地址（在不同网段，假设分别为 192.168.1.1/24 和 192.168.2.6/24）。在这里假设 RouterA、RouterB 和 RouterC 与 RouterD 相连的接口为三层接口，所以 RouterD 上的三个 LAN 接口需要以不带标签方式的 Hybrid 接口类型加入 VLAN 10，也可以配置为带 VLAN 标签方式的 Hybrid 类型接口。

```
<Huawei> system-view
[Huawei] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] vlan 10
[DHCP Server] interface ethernet 5/0/1
[DHCP Server-Ethernet5/0/1] port link-type hybrid
[DHCP Server-Ethernet5/0/1] port hybrid untagged vlan 10
[DHCP Server-Ethernet5/0/1] port hybrid pvid vlan 10
[DHCP Server-Ethernet5/0/1] quit
[DHCP Server] interface ethernet 5/0/2
[DHCP Server-Ethernet5/0/2] port link-type hybrid
[DHCP Server-Ethernet5/0/2] port hybrid untagged vlan 10
[DHCP Server-Ethernet5/0/2] port hybrid pvid vlan 10
[DHCP Server-Ethernet5/0/2] quit
[DHCP Server] interface ethernet 5/0/3
[DHCP Server-Ethernet5/0/3] port link-type hybrid
[DHCP Server-Ethernet5/0/3] port hybrid untagged vlan 10
[DHCP Server-Ethernet5/0/3] port hybrid pvid vlan 10
[DHCP Server-Ethernet5/0/3] quit
[DHCP Server] interface gigabitEthernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface vlanif 10
[DHCP Server-Vlanif10] ip address 192.168.2.6 255.255.255.0
[DHCP Server-Vlanif10] dhcp select global
[DHCP Server-Vlanif10] quit
```

然后在 RouterD 上配置用于为 RouterA、RouterB 和 RouterC 分配 IP 地址信息的全局地址池（地址段为 192.168.2.0/24），并配置 Option 67（配置 DHCP 客户端配置文件）、

141（配置 FTP 用户名）、142（配置 FTP 用户密码）、143（配置 FTP 服务器 IP 地址）、145（配置 DHCP 客户端非配置文件信息）。

```
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 192.168.2.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 192.168.2.6
[DHCP Server-ip-pool-auto-config] option 67 ascii ar_V200R003C00.cfg
[DHCP Server-ip-pool-auto-config] option 141 ascii user
[DHCP Server-ip-pool-auto-config] option 142 ascii huawei
[DHCP Server-ip-pool-auto-config] option 143 ip-address 192.168.1.6
[DHCP Server-ip-pool-auto-config] option 145 ascii vrpfile=ar_V200R003C00.cc; vrpver=V200R003C00; patchfile=ar_V200R003C00.pat;
[DHCP Server-ip-pool-auto-config] quit
```

④ 对待配置设备 RouterA、RouterB 和 RouterC 上电启动，Auto-Config 流程开始运行。Auto-Config 流程结束后，登录到待配置设备执行 **display startup** 命令查看设备当前的启动系统软件，启动配置文件和启动补丁文件。以 RouterA 为例。

```
<Huawei> display startup
MainBoard:
  Startup system software:                     flash:/ar_V200R003C00.cc
  Next startup system software:                flash:/ar_V200R003C00.cc
  Backup system software for next startup:     null
  Startup saved-configuration file:            flash:/ar_V200R003C00.cfg
  Next startup saved-configuration file:       flash:/ar_V200R003C00.cfg
  Startup license file:                        null
  Next startup license file:                   null
  Startup patch package:                       flash:/ar_V200R003C00.pat
  Next startup patch package:                  flash:/ar_V200R003C00.pat
  Startup voice-files:                         null
  Next startup voice-files:                    null
```

2.10.7 跨网段 Auto-Config 功能配置示例

本示例的基本拓扑结构如图 2-19 所示，在某企业分支机构 1、2、3 的开局部署场景中，新出厂设备 RouterA、RouterB 和 RouterC 通过 GE0/0/1 接口跨越传输网络连接到设备 RouterD 的接口 GE0/0/2 上。RouterD 作为企业总部的出口网关，跨越三层网络与总部设备 RouterE 相连。现用户希望在 RouterA、RouterB 和 RouterC 加载不同的系统软件、补丁文件和配置文件；同时，为了降低现场配置的人力成本，用户希望能对这些设备实现远程自动配置。

RouterA、RouterB 和 RouterC 的设备信息及待加载的文件信息如下。

① RouterA：MAC 地址为 0018-82C5-AA89，设备序列号 ESN 为 2102310CXK10B6000183，需加载的系统软件名为 auto_V200R001C00.cc，版本号信息为 V200R001C00，补丁文件为 auto_V200R001C00.pat，配置文件为 auto_V200R001C00.cfg。

② RouterB：MAC 地址为 0018-82C5-AA90，设备序列号 ESN 为 2102310CXK10B6000184，需加载的系统软件名为 auto_V200R002C00.cc，版本号信息为 V200R002C00，补丁文件为 auto_V200R002C00.pat，配置文件为 auto_V200R002C00.cfg。

③ RouterC：MAC 地址为 0018-82C5-AA91，设备序列号 ESN 为 2102310CXK10B6000185，需加载的系统软件名为 auto_V200R003C01.cc，版本号信息为 V200R003C01，补丁文件为 auto_V200R003C01.pat，配置文件为 auto_V200R003C01.cfg。

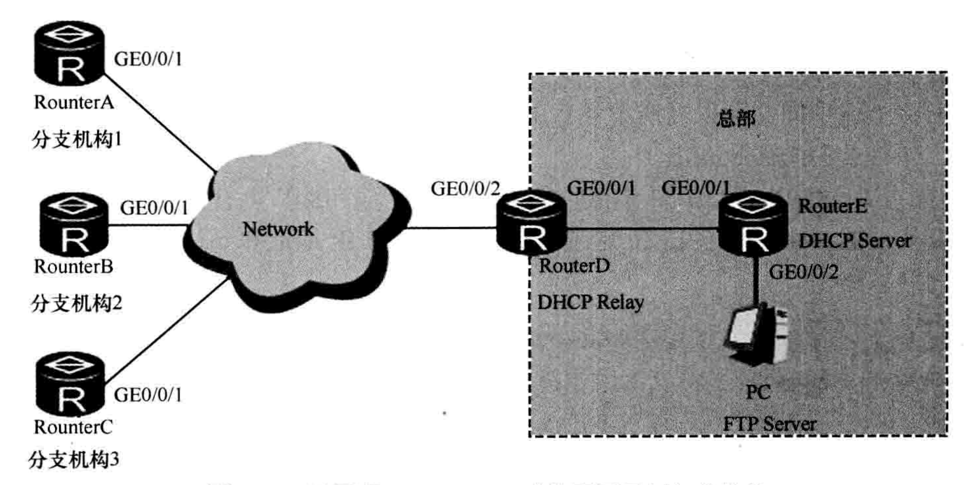


图 2-19　跨网段 Auto-Config 功能配置示例拓扑结构

1. 基本配置思路分析

本示例中待配置的设备所需加载的信息各不一样，所以不能通过 DHCP Option 67 来进行统一配置，需采用中间文件的方式进行配置。整个配置思路如下。

① 用户 PC 与 RouterE 直接相连，在 PC 上配置 FTP 服务器。

② 编辑中间文件，实现待配置设备 RouterA、RouterB 和 RouterC 通过中间文件获取配置文件、系统软件和补丁文件。

③ 将中间文件、系统软件、补丁文件和配置文件放至 FTP 服务器的工作目录下，保证待配置设备能够获取到需要加载的文件。

④ 在企业总部的出口网关设备 RouterD 上配置 DHCP 中继功能；在位于总部的设备 RouterE 上配置 DHCP 服务器。实现 DHCP 服务器跨网段为待配置设备提供网络配置信息。

⑤ RouterA、RouterB 和 RouterC 上电，实现通过 Auto-Config 功能自动加载配置文件、系统软件和补丁文件。缺省情况下，设备的 Auto-Config 功能处于使能状态。

2. 具体配置步骤

① 配置 FTP 服务器的 IP 地址、用户名、密码及工作目录。

同样以 wftpd32 FTP 服务器软件为例，在如图 2-18 所示的对话框中依次选择"Security"→"Uers/rights"。在弹出的对话框中单击"New User…"，设置用户名为 **user**、密码为 **huawei**。在"Home Directory:"文本框处设置 PC 上 FTP 的工作目录为 D:\autoconfig。然后单击"Done"按钮完成设置并关闭对话框。配置 PC 的 IP 地址为 192.168.4.6，掩码为 255.255.255.0。

② 编辑中间文件 arnet.ini。

在一 PC 的文本编辑软件中新建一个文本文件，命名为"arnet.ini"。为 RouterA、RouterB 和 RouterC 配置设备信息及所要加的文件信息。这个中间文件的内容与格式如下。

```
MAC=0018-82C5-AA89;ESN=2102310CXK10B6000183;vrpfile=auto_V200R001C00.cc;vrpver=V200R001C00;patchfile=auto_V200R001C00.pat;cfgfile=auto_V200R001C00.cfg;
MAC=0018-82C5-AA90;ESN=2102310CXK10B6000184;vrpfile=auto_V200R002C00.cc;vrpver=V200R002C00;patchfile
```

```
=auto_V200R002C00.pat;cfgfile=auto_V200R002C00.cfg;
    MAC=0018-82C5-AA91;ESN=2102310CXK10B6000185;vrpfile=auto_V200R003C01.cc;vrpver=V200R003C01;patchfile
=auto_V200R003C01.pat;cfgfile=auto_V200R003C01.cfg;
```

然后将上述中间文件以及所要加载的配置文件、系统软件和补丁文件上传到 FTP 服务器的工作目录 D:\autoconfig 上。

③ 配置 RouterD 的 DHCP 中继功能。包括在全局和接口上使能 DHCP 中继功能，配置所要代理的 DHCP 服务器 IP 地址，并配置各接口 IP 地址和到达 FTP 服务器主机所在网段的静态路由。

```
<Huawei> system-view
[Huawei] sysname DHCP Relay
[DHCP Relay] dhcp enable
[DHCP Relay] interface gigabitethernet 0/0/2
[DHCP Relay-Gigabitethernet0/0/2] ip address 192.168.1.6 255.255.255.0
[DHCP Relay-Gigabitethernet0/0/2] dhcp select relay
[DHCP Relay-Gigabitethernet0/0/2] dhcp relay server-ip 192.168.2.6
[DHCP Relay-Gigabitethernet0/0/2] quit
[DHCP Relay] interface gigabitethernet 0/0/1
[DHCP Relay-Gigabitethernet0/0/1] ip address 192.168.2.1 255.255.255.0
[DHCP Relay-Gigabitethernet0/0/1] quit
[DHCP Relay] ip route-static 192.168.4.0 255.255.255.0 192.168.2.6
```

④ 配置 RouterE 的 DHCP 服务器功能。包括配置用于为 RouterA、RouterB 和 RouterC 分配 IP 地址的 IP 地址池（网段为 192.168.1.0/24），以及 Option 141、142、143、146（配置用户指定动作的操作信息）和到达 192.168.1.0/24 网段的静态路由，但不需要配置用来指定配置文件的 Option 67 和用来指定要加的非配置文件信息的 Option 145，因为设备和配置文件信息已通过中间文件进行了配置。

```
<Huawei> system-view
[Huawei] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] interface GigabitEthernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] ip address 192.168.2.6 255.255.255.0
[DHCP Server-GigabitEthernet0/0/1] dhcp select global
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface GigabitEthernet 0/0/2
[DHCP Server-GigabitEthernet0/0/2] ip address 192.168.4.1 255.255.255.0
[DHCP Server-GigabitEthernet0/0/2] quit
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 192.168.1.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 192.168.1.6
[DHCP Server-ip-pool-auto-config] option 141 ascii user
[DHCP Server-ip-pool-auto-config] option 142 ascii huawei
[DHCP Server-ip-pool-auto-config] option 143 ip-address 192.168.4.6
[DHCP Server-ip-pool-auto-config] option 146 ascii opervalue=1;delay=0;netfile=arnet.ini;
[DHCP Server-ip-pool-auto-config] quit
[DHCP Server] ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

⑤ 对待配置设备 RouterA、RouterB 和 RouterC 上电启动，Auto-Config 流程开始运行。Auto-Config 流程结束后，登录到待配置设备执行 **display startup** 命令查看设备当前的启动系统软件，启动配置文件和启动补丁文件。以 RouterC 为例。

```
<Huawei> display startup
MainBoard:
```

```
Startup system software:                    flash:/auto_V200R003C01.cc
Next startup system software:               flash:/auto_V200R003C01.cc
Backup system software for next startup:    null
Startup saved-configuration file:           flash:/auto_V200R003C01.cfg
Next startup saved-configuration file:      flash:/auto_V200R003C01.cfg
Startup license file:                       null
Next startup license file:                  null
Startup patch package:                      flash:/auto_V200R003C01.pat
Next startup patch package:                 flash:/auto_V200R003C01.pat
Startup voice-files:                        null
Next startup voice-files:                   null
```

第3章
接口配置与管理

3.1 路由器接口基础及基本参数配置与管理

3.2 以太网接口配置与管理

3.3 Serial接口配置与管理

3.4 CE1/PRI接口配置与管理

3.5 E1-F接口配置与管理

3.6 CT1/PRI接口配置与管理

3.7 T1-F接口配置与管理

3.8 3G Cellular接口配置与管理

3.9 POS接口配置与管理

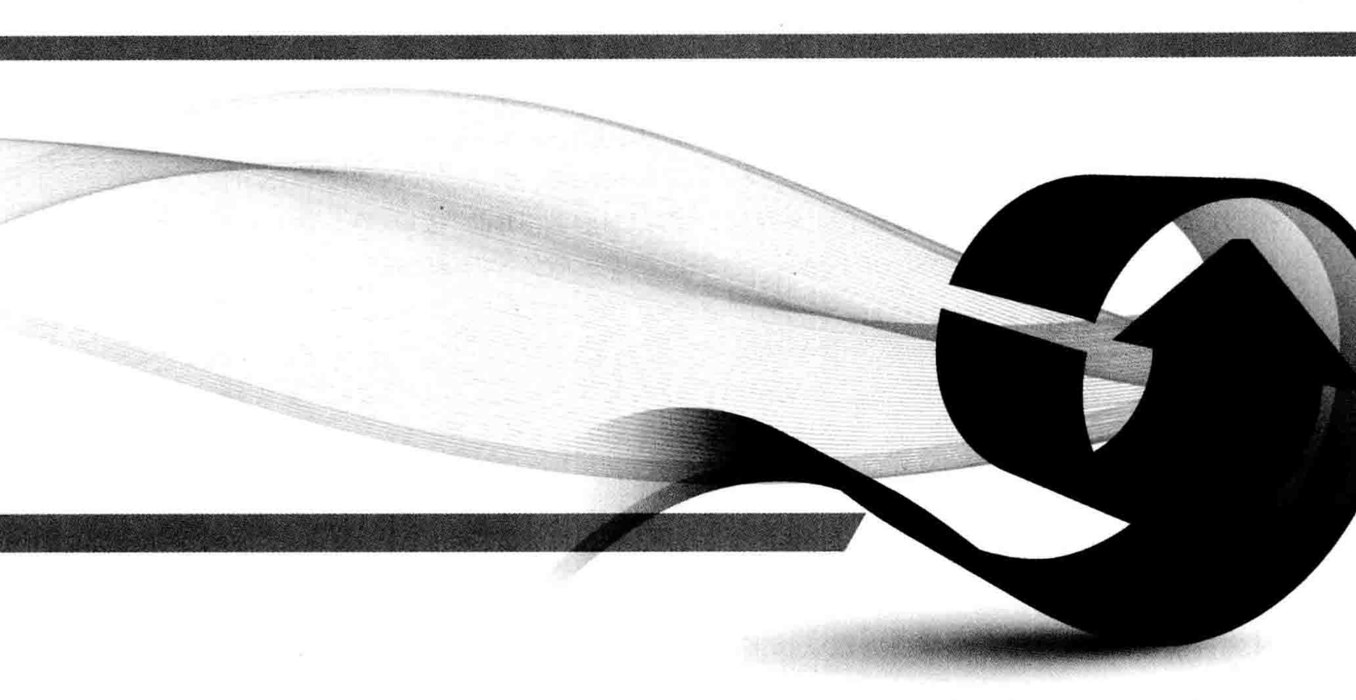
3.10 CPOS接口配置与管理

3.11 PON接口配置与管理

3.12 ADSL接口配置与管理

3.13 VDSL接口配置与管理

3.14 G.SHDSL接口配置与管理



路由器的接口相对于交换机接口来说最大的特点就是接口类型和配置更为复杂。一般可以把路由器上的接口分为三大类：一类是用于局域网组网的LAN接口，另一类是用于广域网接入/互联的WAN接口，最后一类可以应用于LAN组网，或者WAN接入/互联网中的逻辑接口。其中最为复杂的就是各种WAN接口。

本章将介绍华为AR G3系列路由器中的各种接口的配置与管理，侧重于各种WAN接口配置，主要包括Serial接口、Async接口、CE1/PRT接口、E1–F接口、CT1/PRI接口、T1–F接口、3G Cellular接口、POS接口、CPOS接口、PON接口、ADSL接口、VDSL接口和G.SHDSL接口等。它们都对相应的WAN接入或者连接方式提供支持，大家要着重理解各种接口的用途及其基本配置任务。

注意 在以上这么多WAN接口中，有些接口直接通过本章介绍的配置即可实现对应的WAN接入/互联，这些都是用于各种专线接入的WAN接口，如用于E1专线接入的CE1/PRT接口和E1-F接口，用于T1专线接入的CT1/PRI接口和T1-F接口，用于SONET/SDH网络接入的POS接口和CPOS接口，用于EPON/GPON网络接入的PON接口等。而有些仅配置好了对应的接口还不能实现对应的WAN接入/互联，这些一般是按需拨号的接口，如3G Cellular接口、ADSL接口、VDSL接口和G.SHDSL接口等。要实现这些拨号方式的WAN接入/互联，则还需进行相关的链路层协议及拨号配置（如DCC配置），具体将在下章介绍。还有些可同时应用于直接的WAN互联和WAN拨号连接，如Serial接口、Async接口等。

3.1 路由器接口基础及基本参数配置与管理

路由器与交换机相比，外观上看最明显的特点就是接口类型繁多，不仅包括了各种局域以太网接口，更包括用于各种广域网连接的接口，如 Serial 接口、E1 专线的 CE1/RPI 接口/E1-F 接口，T1 专线的 CT1/RPI 接口/T1-F 接口、3G 无线的 3G Cellular 接口、SONET/SDH 的 POS 接口/CPOS 接口、ADSL 接口、VDSL 接口、G.SHDSL 接口、EPON 和 GPON 的 PON 接口，还有各种逻辑接口，如 Loopback 接口、NULL 接口、Dialer 接口、VE 接口、VT 模板和 MP-Group 接口等。当然，并不是在一台路由器中包括全部的这些接口。

3.1.1 接口分类

接口是设备与网络中的其他设备交换数据并相互作用的部件。在 AR G3 系列路由器中，所有接口共分为管理接口、物理接口和逻辑接口三大类。

1. 管理接口

管理接口主要为用户提供配置管理支持，也就是用户通过此类接口可以登录到设备，并进行配置和管理操作，**但管理接口不承担业务传输**。

AR G3 系列路由器支持 Console 和 Mini-USB 两种管理接口，但它们互斥，即同一时刻只能使用其中的 1 个接口。默认情况下，Console 接口为串行接口。关于这两种管理接口的说明如表 3-1 所示。

表 3-1 AR G3 系列路由器支持的管理接口

接口名称	说明
Console 口	遵循 EIA/TIA-232 标准，DCE 类型，用于与配置终端的 COM 串口连接，进行设备本地登录和配置
MiniUSB 口	遵循 USB1.0 标准，用于通过 MiniUSB 线缆与终端的 USB 口建立物理连接，进行设备本地登录和配置

2. 物理接口

物理接口是真实存在、有器件支持的接口，需要承担业务传输。物理接口有时也被称为端口，为便于描述，在本书中，统一描述为接口。物理接口分为两种。

① LAN 接口：路由器可以通过它们与局域网中的网络设备交换数据。

② WAN 接口：路由器可以通过它们与局域网外的网络设备交换数据。

AR G3 系列路由器所支持的物理接口如表 3-2 所示。

表 3-2 AR G3 系列路由器所支持的物理接口类型

接口种类	接口类型	说明
LAN 接口	FE/GE 接口	工作在数据链路层，处理二层协议，实现二层数据转发，最大速率分别为 100 Mbit/s、1 000 Mbit/s
WAN 接口	FE/GE 接口	工作在网络层，可配置 IP 地址，处理三层协议，提供路由功能，最大速率分别为 100 Mbit/s、1 000 Mbit/s
	Serial 接口	同异步串口，可工作在同步或异步模式。在同步串口上支持配置 PPP、FR 等链路层协议和 IP 地址；在协议模式下的异步串口上还支持 PPP 数据链路层协议和 IP 地址（**流模式下不支持**）

（续表）

接口种类	接口类型	说明
WAN 接口	Async 接口	异步专线串口，协议模式下的 Async 接口上支持 PPP 数据链路层协议和 IP 地址（**流模式下不支持**）
	CE1/CT1 接口	通道化 E1/T1 接口，可配置 IP 地址，处理三层协议，逻辑特性和同步串口相同，可配置接口工作在不同的工作模式下，以支持 PPP、FR、ISDN 等应用
	E1-F/T1-F 接口	部分通道化 E1/T1 接口，分别是 CE1/PRI 或 CT1/PRI 接口的简化版本，可满足简单的 E1/T1 接入需求
	ADSL 接口	利用普通电话线中未使用的高频段，能在一对普通铜双绞线上提供**不对称**的上下行速率，实现数据的高速传输
	G. SHDSL 接口	利用了普通电话线中未使用的高频段，能在一对普通铜双绞线上提供**对称**的上下行速率，实现数据的高速传输
	VDSL 接口	是在 DSL 的基础上集成各种接口协议，通过复用上传和下传管道以获取更高的传输速率
	E1-IMA 接口	用于将 ATM 信元分接到 E1-IMA 链路上直接传输
	3G Cellular 接口	用于 3G 无线接入，数据链路层使用 PPP，网络层使用 IP
	ISDN BRI 接口	ISDN 基本速率接口，接入 ISDN，提供带宽为 64 kbit/s 或 128 kbit/s 的连接（包括两个 64 kbit/s 的 B 信道和一个 16 kbit/s 的 D 信道）。可配置 IP 地址，支持配置 PPP、FR 等链路层协议
	POS 接口	使用 SONET/SDH 物理层传输标准，提供一种高速、可靠、点到点的 IP 数据连接
	CPOS 接口	通道化的 POS 接口，汇聚 SONET/SDH 传输网的 E1/T1 线路
	语音接口	语音接口分为以下几种。 ● FXS（外部交换站）端口：用于和模拟电话连接。为了使 FXS 端口传输效果达到最优，设备提供 FXS 端口参数配置，包括物理属性、电气属性 ● FXO（外部交换局）端口：主要用于和 PSTN（公共交换电话网）互联。为了使 FXO 端口传输效果达到最优，设备提供 FXO 端口参数配置，包括增益、阻抗、铃流、馈电 ● BRA（基准速率）端口：主要用于连接 ISDN 话机。设备提供 BRA 端口参数配置，包括 BRA 端口 L2 监视功能、端口工作模式、远供功能、自动去激活功能、端口 L1 激活方式、故障告警功能 ● VE1（高密度语音）端口：通常用于和 PBX（用户电话交换机）或 PSTN 互联。设备提供 VE1 端口参数配置，包括 CRC4 校验、CRC 告警门限、E1 端口 L2 监视、E1 端口 PCM 告警、E1 端口的信令模式

3. 逻辑接口

逻辑接口是指能够实现数据交换功能，承担业务传输，但物理上不存在，需要通过配置建立的虚拟接口。AR G3 系列路由器所支持的逻辑接口如表 3-3 所示。

表 3-3　AR G3 系列路由器支持的逻辑接口

接口类型	说明
Eth-Trunk 接口	具有二层特性和三层特性的逻辑接口，把多个以太网接口在逻辑上等同于一个逻辑接口，比以太网接口具有更大的带宽和更高的可靠性
VT（Virtual-Template，虚拟接口模板）接口	当需要 PPP 承载其他链路层协议时，可通过配置虚拟接口模板来实现

（续表）

接口类型	说明
VE（Virtual-Ethernet，虚拟以太网）接口	主要用于以太网协议承载其他数据链路层协议
MP-Group 接口	MP（多链路 PPP）的专用接口，可实现多条 PPP 链路的捆绑，通常应用在那些具有动态带宽需求的场合
Dialer 接口	配置 DCC（拨号控制中心）参数而设置的逻辑接口，物理接口可以绑定到 Dialer 接口以继承配置信息
Tunnel 接口	具有三层特性的逻辑接口，隧道两端的设备利用 Tunnel 接口发送报文、识别并处理来自隧道的报文
VLANIF 接口	具有三层特性的逻辑接口，通过配置 VLANIF 接口的 IP 地址，实现 Vlan 间互访
子接口	是在一个主接口上配置出来的虚拟接口，主要用于实现与多个远端进行通信
MFR 接口	当一条物理链路的带宽不能满足需求时，可以使用将多条物理链路（包括通道化的串口）捆绑成一条链路，形成一个 MFR 接口，以提供更大的带宽
Loopback 接口	主要应用其接口可以配置 32 位子网掩码的特性
NULL 接口	任何发送到该接口的网络数据报文都会被丢弃，主要用于路由过滤等特性
Bridge 接口	具有三层特性的逻辑接口，通过配置 Bridge 接口的 IP 地址，实现透明网桥中不同网段间用户的互访
IMA 组	IMA（ATM 反向复用）组是由一条或多条 E1-IMA 链路组成的逻辑链路，提供更高带宽（近似等于所有成员链路的带宽之和），使多个低速链路复用起来支持高速 ATM 信元流
WLAN-Radio 接口	WLAN-Radio 接口是一种逻辑接口，可以进行射频的相关配置
WLAN-BSS 接口	WLAN-BSS 是一种虚拟的二层接口，类似于 Access 类型的二层以太网接口，具有二层属性，并可配置多种二层协议

说明 由于篇幅限制，在本章不可能对以上各种类型的接口进行全面介绍，仅介绍应用最广的一些接口，如以太网接口、Searial 接口、CE1/PRI 接口、CT1/PRI 接口、E1-F 接口、T1-F 接口、POS 接口、CPOS 接口、PON 接口、3G Cellular 接口、ADSL 接口、G.SHDSL 接口、VDSL 接口等广域网物理接口，以及 VT、VE、MP-Group 和 Dialer 等这些逻辑接口。

3.1.2 物理接口编号规则

前面说了，物理接口是实际存在的接口，这就需要为每个接口配置一个编号，以标识每个接口。AR G3 系列路由器采用“槽位号/子卡号/接口序号”的格式来定义接口编号。

① 槽位号：表示接口所在的路由器单板所在的槽位号。

这里首先要明白两个概念，一是什么是“单板”，二是什么是“主控板”，这两个术语在本书后面，以及在看一些网络设备资料时经常会见到。

“单板”可以理解为单一功能板，是插在主控板上面，用于实现某种功能的电路板（也称接口卡，或者模块），如我们通过插入某一个功能模块（如各种类型以太网接口卡），则这个模块电路板就是一个单板。“主控板”是路由器系统控制和管理的核心，提供整个系统的控制平面，管理平面和业务交换平面，通常还包括电源和风扇模块。

一般来说，一台路由器设备只有一个主控板，但在一些高端路由器设备中也可能有多个主控板，如 NE40E 系列路由器最多就可以安装两个主控板。

因为 AR150/150-S/160/200/200-S 系列、AR1200/AR1200-S 系列、AR2201-48FE、AR2202-48FE、AR2204、AR2220L、AR2201-48FE-S、AR2204-S 和 AR2220-S 和 AR2220S 的主控板是一体化的（没有单板），且只有一个主控板，所以其主控板物理槽位号统一取值为 0。

其他系列和机型的各单板槽位号遵照产品手册说明，遇到槽位合并时，物理槽位号取较大槽位编号，举例：槽位 1 和槽位 2 合并后，取新槽位号 2。

② 子卡号：表示各单板上所插入的子卡编号。但因为 AR G3 系列路由器各单板都不支持子卡，因此统一取值为 0。也正因如此，AR G3 系列路由器各接口编号中的第二位均为 0。

③ 接口序号：表示各主控板和单板上各接口的编排顺序号。

如果接口板面板上只有一排接口，则最左侧接口从 0 起始编号，其他接口从左到右依次递增编号，如图 3-1 所示。

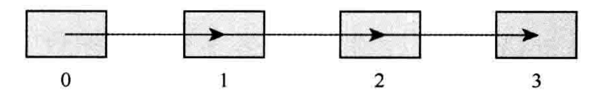


图 3-1　单排接口子卡上的接口编号顺序

如果接口板面板上有两排接口（路由器上的接口，只是类型多，数量不会太多，所以一般不会超过两排的），则左下接口从 0 起始编号，其他接口从下到上，再从左到右依次递增编号，如图 3-2 所示。很好记，下面一排全为偶数（最左边的接口序号为 0）0、2、4、6、8，上面一排全为奇数（最左边的接口序号为 1），1、3、5、7、9。

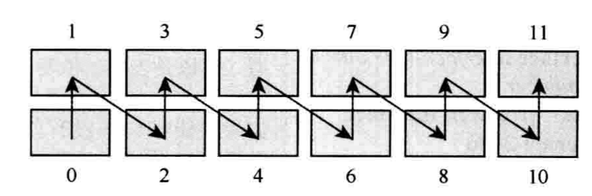


图 3-2　双排接口子卡上的接口编号顺序

3.1.3　接口基本参数配置

在 AR G3 系列路由器中，可以配置以下接口基本参数。

1. 配置接口描述信息

为了方便管理和维护设备，可以配置接口的描述信息，如描述接口所属的设备、接口类型，或者对端所连接的设备等信息。例如："当前设备连接到设备 B 的 Eth2/0/0 接口"可以描述为：To-[DeviceB]Eth-2/0/0。

2. 配置流量统计时间间隔

通过配置接口的流量统计时间间隔功能，用户可以精确地对某个时间段感兴趣的报文进行统计与分析，以便必要时及时对接口采取流量控制的措施，避免网络拥塞和业务中断。

一般来说，当用户发现网络有拥塞时，可将接口的流量统计时间间隔设置为小于300 s（拥塞加剧时可设为 30 s）；当业务运行正常时，可将接口的流量统计时间间隔设置为大于 300 s。一旦发现流量异常，及时修改流量统计时间间隔，便于更实时地观察该流量参数的趋势。

流量统计时间间隔可以在系统视图下对设备上的所有接口进行全局配置，应用于所有采用缺省配置的接口；也可在接口视图下单独为某一个接口配置，仅对本接口生效，不影响其他接口。在接口视图下配置时间间隔的优先级高于在系统视图下配置的时间间隔。

3. 配置开启或关闭接口

当修改了接口的工作参数配置，新的配置未能立即生效，此时需要依次执行 **shutdown** 和 **undo shutdown** 命令或 **restart** 命令关闭和重启接口，使新的配置生效。当接口闲置（即没有连接电缆或光纤）时，请使用 **shutdown** 命令关闭该接口，以防止由于干扰导致接口异常。

说明 依次执行 **shutdown** 和 **undo shutdown** 命令相当于执行 **restart** 命令，不会修改或删除接口的配置信息。

NULL 接口一直处于 Up 状态，不能使用命令关闭或启动 NULL 接口。Loopback 接口一旦被创建，也将一直保持 Up 状态，也不能使用命令关闭或启动 Loopback 接口。

以上配置任务的具体配置步骤如表 3-4 所示（但需要先进入接口视图），但各项配置任务没有严格的配置顺序，表中的配置步骤序号仅为方便介绍。

表 3-4 接口基本参数配置步骤

配置任务	步骤	命令	说明
进入接口视图	1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
	2	**interface** *interface-type interface-number* 例如：[Huawei] **interface ethernet** 2/0/0	进入接口视图。其中，*interface-type* 为接口类型（可以是表 3-2 和表 3-3 中列出的各种接口），*interface-number* 为接口编号 如果逻辑接口还没有创建，则此命令用于创建逻辑接口并进入该逻辑接口视图
配置接口描述信息	3	**description** *description* [Huawei-Ethernet2/0/0] **description** To-[DeviceB] Eth-2/0/0	配置接口的描述信息，1～242 个字符，支持空格，区分大小写，但字符串中不能包含“?”。**描述信息把输入的第一个非空格字符作为第一个字符开始显示** 缺省情况下，接口描述信息为“HUAWEI, AR Series, *interface-type interface-number* Interface ”，可用 **undo description** 命令恢复接口描述信息为缺省情况
配置接口流量统计时间间隔	4	**基于接口配置：** [Huawei-Ethernet2/0/0] **set flow-stat interval** 400 **基于全局配置：** **set flow-stat interval** *interval-time* 例如：[Huawei] **set flow-stat interval** 400	基于接口配置（**必须在对应的接口视图下配置**）或者全局配置（**必须在系统视图下配置**）接口流量统计时间间隔，取值范围为 10～600 的整数秒，但取值必须是 10 的整数倍 缺省情况下，接口的流量统计时间间隔为 300 s，可用 **undo set flow-stat interval** 命令恢复接口的流量统计时间间隔为缺省值

（续表）

配置任务	步骤	命令	说明
关闭接口或开启接口	5	**shutdown** 例如：[Huawei-Ethernet2/0/0] **shutdown** 或 **undo shutdown** 例如：[Huawei-Ethernet2/0/0] **undo shutdown**	关闭接口或开启接口。缺省情况下，接口处于打开状态 【说明】**在 Eth-Trunk 接口视图下执行 shutdown 命令，则其中所有成员接口都将被关闭。**当接口下配有子接口时，缺省情况下，在主接口下依次执行 **shutdown** 和 **undo shutdown** 操作的间隔为 15 s，可通过 **shutdown interval** 命令修改间隔时间

3.1.4　接口基本参数配置管理

可以通过以下 **display** 任意视图命令和 **reset** 用户视图命令对接口基本配置信息进行管理。

① **display interface** [*interface-type* [*interface-number*]]：查看所有或者指定接口当前运行状态信息，包括接口当前运行状态、接口基本配置和报文通过接口的转发情况。

② **display interface brief**：查看所有接口状态和配置的简要信息，包括接口的物理状态、协议状态、接收方向最近一段时间的带宽利用率、发送方向最近一段时间的带宽利用率、接收的错误报文数和发送的错误报文数。

③ **display ip interface** [*interface-type interface-number*]：查看所有或者指定接口的主要 IP 配置信息。

④ **display default-parameter interface** *interface-type interface-number*：查看指定接口缺省配置。

⑤ **display interface description** [*interface-type* [*interface-number*]]：查看所有或者指定接口的描述信息。

⑥ **display interface** [*interface-type*] **counters** { **inbound** | **outbound** }：查看所有或者指定物理接口发送或接收报文的统计信息。

⑦ **display transceiver** [**interface** *interface-type interface-number* | **controller** *controller-type controller-number* | **slot** *slot-id*] [**verbose**]：查看所有或者指定接口上的光模块信息。

⑧**reset counters interface** [*interface-type* [*interface-number*]]：清除所有或者指定接口的统计信息。

⑨ **reset counters if-mib interface** [*interface-type* [*interface-number*]]：清除网管的接口流量统计信息。

3.2　以太网接口配置与管理

在 AR G3 系列路由器中都是带有一定数量 LAN、WAN 以太网接口的，用于局域网的组网和以太广域网的连接。以太网接口根据其使用的传输介质又分为以太网电接口和以太网光接口。

3.2.1 以太网接口分类

以太网接口根据其工作的网络体系架构层次可分为二层以太网接口和三层以太网接口两种。

① 二层以太网接口：工作在数据链路层，不能配置 IP 地址，可以对接收到的报文进行二层交换转发，也可以加入 VLAN，通过 VLANIF 接口对接收到的报文进行三层路由转发。二层以太网接口属性如表 3-5 所示。

表 3-5 二层以太网接口的属性

<table>
<tr><th>接口类型</th><th>速率（Mbit/s）</th><th>双工模式</th><th>自动协商模式</th><th>流量控制</th><th>流量控制自动协商</th></tr>
<tr><td rowspan="2">FE 电接口</td><td>10</td><td>全双工/半双工</td><td rowspan="2">支持</td><td rowspan="2">支持</td><td rowspan="2">不支持</td></tr>
<tr><td>100</td><td>全双工/半双工</td></tr>
<tr><td rowspan="3">GE 电接口</td><td>10</td><td>全双工/半双工</td><td rowspan="3">支持</td><td rowspan="3">支持</td><td rowspan="3">支持</td></tr>
<tr><td>100</td><td>全双工/半双工</td></tr>
<tr><td>1 000</td><td>全双工</td></tr>
<tr><td rowspan="2">GE 光接口</td><td>100</td><td>全双工</td><td rowspan="2">支持</td><td rowspan="2">支持</td><td rowspan="2">支持</td></tr>
<tr><td>1 000</td><td>全双工</td></tr>
</table>

② 三层以太网接口：工作在网络层，可以配置 IP 地址，可以对接收到的报文进行三层路由转发。三层以太网接口属性如表 3-6 所示。

表 3-6 三层以太网接口的属性

<table>
<tr><th>接口类型</th><th>速率（Mbit/s）</th><th>双工模式</th><th>自动协商模式</th><th>流量控制</th><th>流量控制自动协商</th></tr>
<tr><td rowspan="2">FE 电接口</td><td>10</td><td>全双工/半双工</td><td rowspan="2">支持</td><td rowspan="2">支持</td><td rowspan="2">不支持</td></tr>
<tr><td>100</td><td>全双工/半双工</td></tr>
<tr><td rowspan="3">GE 电接口</td><td>10</td><td>全双工/半双工</td><td rowspan="3">支持</td><td rowspan="3">支持</td><td rowspan="3">支持</td></tr>
<tr><td>100</td><td>全双工/半双工</td></tr>
<tr><td>1 000</td><td>全双工</td></tr>
<tr><td rowspan="2">GE 光接口</td><td>100</td><td>全双工</td><td rowspan="2">支持</td><td rowspan="2">支持</td><td rowspan="2">支持</td></tr>
<tr><td>1 000</td><td>全双工</td></tr>
</table>

二层和三层以太网接口都有电接口和光接口两类，电接口包括 FE 电接口和 GE 电接口，光接口包括 GE 光接口。其中，AR1200/1200-S/2200/2200-S/3200 系列都同时支持 FE 电接口、GE 电接口和 GE 光接口，**AR150/150-S/200/200-S 系列仅支持 FE 电接口，AR160 系列仅支持 GE 电接口。**

缺省情况下，AR150/150-S/200/200-S 系列的 Ethernet0/0/0 接口，AR160 系列的 GE0/0/0 接口，AR2201-48FE/2201-48FE-S/2202-48FE 中的 Ethernet0/0/0 和 Ethernet0/0/47 接口均为二层模式（其他接口均为三层模式），支持通过 **undo portswitch** 命令从二层模式切换到三层模式。

以太网接口常见参数的缺省配置如表 3-7 所示。

表 3-7 以太网接口缺省配置

参数	缺省值
Combo 接口工作模式	电口模式，即使用网线传输数据
MDI 类型	Auto，即自动识别所连接网线的类型
双工模式	自动协商模式下，接口的双工模式是与对端协商得到的；非自动协商模式下，接口的双工模式为全双工
接口速率	自动协商模式下，接口的速率是与对端协商得到的；非自动协商模式下，接口的速率为接口支持的最大速率

3.2.2 配置以太网接口基本属性

在 AR G3 系列路由器中，以太网接口的配置主要包括以下几个方面，其中大多数配置方法与华为 S 系列园区交换机中的以太网接口配置方法完全一样，可直接参见配套图书《华为交换机学习指南》第 4 章相关内容。

1. 端口组配置

当用户需要对多个以太网接口进行相同的配置时，可以将这多个以太网接口加入端口组内。这样，在端口组视图下，用户只需输入一次配置命令，该端口组内的所有以太网接口都会配置该功能，完成接口批量配置，减少了重复配置工作。

可以配置以下两种端口组：永久端口组和临时端口组。这两种端口组功能相同，不同之处仅在于，当所有接口退出临时端口组后，该临时端口组将被系统自动删除，而永久端口组不会这样。

以上两种端口组的具体配置方法**参见《华为交换机学习指南》第 4 章 4.2.2 小节**，只是在 AR G3 系列路由器中，在临时端口组和永久端口组中最多只能添加 5 个以太网端口或端口范围，毕竟路由器上的 LAN 以太网接口不像交换机上那么多。

2. 以太网接口基本属性配置

这个方面主要是包括以太网接口（包括二层以太网接口和三层以太网接口）的通用基本配置，例如接口速率、自动协商、MDI 类型、双工模式、电缆检测、流量控制等属性配置。这些方面的配置请**参见《华为交换机学习指南》第 4 章 4.2.3 小节**。

在 AR G3 系列路由器基本配置方面，还包括一项“出/入带宽利用率日志和告警阈值”配置。通过查看设备接口的带宽利用率能够了解当前设备的负载，如果带宽利用率超过一定阈值，则表明带宽资源已经难以满足当前的业务需求，急需对设备进行扩容。

可以对设备设置两级阈值，低阈值（日志阈值）产生日志提示，高阈值（告警阈值）产生告警提示，保证用户可以提前扩容，避免因为带宽耗尽造成业务中断。低阈值取值要低于高阈值取值，以保证对业务的双重保护。例如，入带宽的低阈值设置为 80%，入带宽的高阈值设置为 95%，就可以保证在入带宽利用率达到 80%的时候通过日志提示用户需要扩容，在达到 95%的时候会通过告警再次提示用户，避免业务中断。

出/入带宽利用率日志和告警阈值的具体配置步骤如表 3-8 所示。

表 3-8 以太网接口出/入带宽利用率日志和告警阈值的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** ethernet 2/0/0	键入要配置出/入带宽利用率日志和告警阈值的接口，进入接口视图
3	**log-threshold** { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume -rate** *resume-threshold*] 例如：[Huawei-Ethernet2/0/0] **log-threshold output-rate** 80 **resume-rate** 60	配置接口的入、出带宽利用率日志阈值，也就是配置在带宽利用率到达什么水平时产生日志。命令中的参数和选项说明如下 ● **input-rate**：二选一选项，指定配置入带宽利用率日志阈值 ● **output-rate**：二选一选项，指定配置出带宽利用率日志阈值 ● *bandwidth-in-use*：指定产生日志的入或出带宽利用率阈值，取值范围是 1～100 的整数，相当一个百分比。相当于当接口带宽利用率到达这个值后即产生日志记录 ● **resume-rate** *resume-threshold*：可选参数，指定产生恢复日志的入或出带宽利用率阈值，取值范围是 1～*bandwidth-in-use*，缺省值等于 *bandwidth-in-use*，通常是小于 *bandwidth-in-use*，也相当于一个百分比。带宽利用率从产生日志的带宽利用率阈值以上降到恢复日志的带宽利用率阈值以下，系统将产生日志恢复信息。为了避免日志信息震荡，*bandwidth-in-use* 和 *resume-threshold* 的取值尽量保持差距 【说明】出带宽利用率＝（接口出流量速率/接口所在物理接口的带宽）×100；入带宽利用率＝（接口入流量速率/接口所在物理接口的带宽）×100 缺省情况下，接口出、入带宽利用率的日志阈值是 100，可用 **undo log-threshold** { **input-rate** | **output-rate** }命令用来恢复接口入、出带宽利用率的日志阈值为缺省值
4	**trap-threshold** { **input-rate** | **output -rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*] 例如：[Huawei-Ethernet2/0/0] **trap-threshold intput-rate** 90 **resume-rate** 70	配置接口的入、出带宽利用率告警阈值，也就是配置在带宽利用率到达什么水平时产生告警。命令中的参数和选项说明如下 ● **input-rate**：二选一选项，指定配置入带宽利用率告警阈值 ● **output-rate**：二选一选项，指定配置出带宽利用率告警阈值 ● *bandwidth-in-use*：指定产生日志的入或出带宽利用率告警阈值，取值范围是 1～100 的整数，相当一个百分比。当带宽利用率超出产生告警的带宽利用率阈值，系统将产生告警信息 ● **resume-rate** *resume-threshold*：可选参数，指定恢复告警的带宽利用率阈值，取值范围是 1～*bandwidth-in-use*，缺省值等于 *bandwidth-in-use*，通常是小于 *bandwidth-in-use*，也相当于一个百分比。带宽利用率从产生告警的带宽利用率阈值以上降到这个恢复告警的带宽利用率阈值以下，系统将产生告警恢复信息。但为了避免告警震荡，*bandwidth-in-use* 和 *resume-threshold* 的取值尽量保持差距 缺省情况下，带宽利用率的告警阈值是 100，可用 **undo trap-threshold** { **input-rate** | **output-rate** }命令恢复接口入、出带宽利用率的告警阈值为缺省值

3. 以太网接口基本配置管理

配置好以上以太网接口基本配置后，可以通过以下 **display** 任意视图命令管理基本配置信息。

① **display interface** [*interface-type* [*interface-number*]]：查看所有或者指定接口当前运行状态信息，包括接口当前运行状态、接口基本配置和报文通过接口的转发情况。

② **display interface brief**：查看接口状态和配置的简要信息，包括接口的物理状态、协议状态、接收方向最近一段时间的带宽利用率、发送方向最近一段时间的带宽利用率、接收的错误报文数和发送的错误报文数。

③ **display interface description** [*interface-type* [*interface-number*]]：查看所有或者指定接口的描述信息。

④ **display interface ethernet brief**：查看以太网接口的简要信息，包括接口的物理状态、自动协商方式、双工模式、接口速率、接口接收方向和发送方向最近一段时间的平均带宽利用率。

⑤ **display error-down recovery** [**interface** *interface-type interface-number*]：查看处于 Error-down 状态的接口的相关信息。

3.2.3 自动协商速率范围配置示例

如图 3-3 所示，PC1、PC2 和 PC3 分别与 RouterA 的 Ethernet2/0/0、Ethernet2/0/1 和 Ethernet2/0/2 相连，通过上行线路接入 Internet 网络。

PC1、PC2 和 PC3 的网卡速率均为 100 Mbit/s，RouterA 与 Internet 网络相连接口 Ethernet2/0/3 的速率也为 100 Mbit/s。通常情况下，设备以太网接口速率是通过和对端自动协商决定的，协商得到的速率可以是接口速率能力范围内的任意一个速率。如果在设备上不指定自动协商速率范围，则接口 Ethernet2/0/0、Ethernet2/0/1 和 Ethernet2/0/2 与 PC1、PC2 和 PC3 速率协商的结果都将为 100 Mbit/s，这样就可能造成 RouterA 的出接口 Ethernet2/0/3 拥塞。

为了避免这种现象，本示例可以把 Ethernet2/0/0、Ethernet2/0/1 和 Ethernet2/0/2 接口均配置为自动协商模式，且指定协商速率为 10 Mbit/s。下面仅以 Ethernet2/0/0 接口的自动协商配置为例进行介绍，Ethernet2/0/1 和 Ethernet2/0/2 接口的配置方法完全一样，参见即可。具体配置步骤如下。

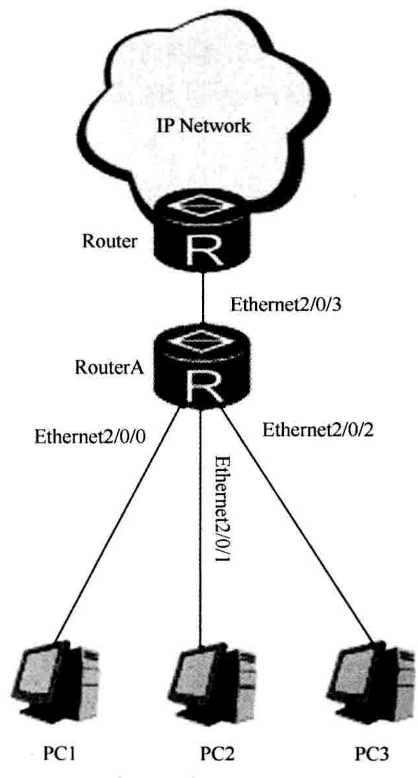


图 3-3　自动协商速率范围配置示例基本网络结构

① 配置 Ethernet2/0/0 接口为速率自动协商模式。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] negotiation auto
```

② 配置 Ethernet2/0/0 接口的自动协商速率为 10 Mbit/s。

```
[RouterA-Ethernet2/0/0] auto speed 10
[RouterA-Ethernet2/0/0] quit
```

3.2.4 配置二层以太网接口

本节将介绍只有二层以太网接口支持的一些配置，包括帧间隙、端口隔离等内容。

1. 端口隔离配置

“端口隔离”就是隔离不同以太网接口的二层通信。在 AR G3 系列路由器中，除了通过传统的 VLAN 划分方式，还有两种方式：配置接口单向隔离和配置端口隔离组。“端口单向隔离”方案可使当前端口与指定的以太网接口进行二层甚至三层隔离，**但是单向的，即仅使当前端口不能发送数据给指定的接口，但不限制这些端口发送数据给当前端口**；“端口隔离组”方案是把想相互隔离的以太网接口加入到同一个隔离组中，使得端口组中的这些以太网接口彼此二层甚至三层隔离。

当希望同一端口隔离组内的用户之间不能二层互通，却可以通过交换机访问公共资源，如打印机、服务器等，可通过配置端口隔离模式为二层隔离三层互通来实现。当希望同一端口隔离组内的用户两两之间二层、三层都不能互通，可通过配置端口的隔离模式为二层、三层都隔离来实现。

关于这两种端口隔离方案及配置方法请**参见《华为交换机学习指南》第 4 章 4.3.1 小节**。

AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2220L、AR2201-48FE-S、AR2201-48FE 和 AR2202-48FE 仅支持二层隔离三层互通，即不支持端口隔离模式配置命令 **port-isolate mode** { **l2** | **all** }中的 **all** 选项（指定端口隔离模式为二层三层都隔离）。4GE-2S、9ES2、4ES2G-S 或 4ES2GP-S 接口卡上的接口不支持跨板端口隔离。

可通过 **display port-isolate group** { *group-id* | **all** }命令查看接口隔离组的配置。

2. 配置帧间隙

以太网帧与帧之间至少要有一定的帧间隙，以便区分两个数据帧。配置以太网帧之间的帧间隙，可以改变包转发率，调整设备接口上的数据包转发能力。

配置帧间隙的方法很简单，仅需在对应接口视图下使用 **ifg** *ifg-value* 命令配置即可，参数 *ifg-value* 用来指定以太网帧之间的帧间隙，取值范围为（9～12）byte。缺省情况下，帧间隙为 12 个字节，可用 **undo ifg** 命令恢复为缺省情况。



AR150/150-S/160/200/200-S/1200/1200-S 系列不支持配置以太网帧之间的帧间隙。

3.2.5 端口隔离配置示例

如图 3-4 所示，PC1、PC2 和 PC3 同属于 VLAN10，用户希望 PC1 与 PC2 之间在 VLAN10 内不能互相访问，PC1 与 PC3 之间可以互相访问，PC2 与 PC3 之间可以互相访问。

本示例要求的是 PC1 与 PC2 之间不能二层互访（没有要求不能三层互访），可以通过端口隔离组方案来实现，不能通过端口单向隔离方案来实现。因为本示例仅要求 PC1 与 PC2 之间不能互访，相当于只需创建一个端口隔离组，且 AR G3 系列路由器缺省情况下的端口隔离模式为二层隔离、三层互通，正好满足本示例要求，所以在本示例中只需要将对应的两个端口上启用隔离功能（缺省都加入到端口隔离组 1 中），就可以实现 PC1 与 PC2 所连端口之间二层数据的隔离，而不用配置隔离模式为 L2 模式。具体的配置步骤如下。

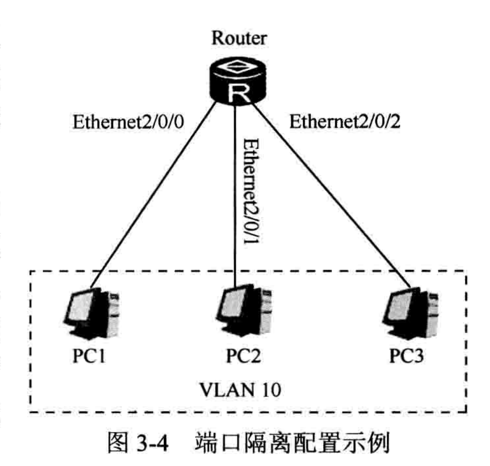


图 3-4　端口隔离配置示例

① 配置 Ethernet2/0/0 的端口隔离功能（不用配置隔离模式，也不用指定加入的隔离组，缺省加入到隔离组 1 中）。

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-isolate enable
[Huawei-Ethernet2/0/0] quit
```

② 配置 Ethernet2/0/1 的端口隔离功能（同样不用配置隔离模式，也不用指定加入的隔离组，缺省加入到隔离组 1 中）。

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port-isolate enable
[Huawei-Ethernet2/0/1] quit
```

最终可以通过 ping 工具来验证配置结果。

- PC1 和 PC2 不能互相 ping 通。
- PC1 和 PC3 可以互相 ping 通。
- PC2 和 PC3 可以互相 ping 通。

3.2.6　配置三层以太网接口

本节将介绍只有三层以太网接口支持的一些配置，包括最大传输单元 MTU（Maximum Transmission Unit）、Combo 接口工作模式等内容。

1. 配置 MTU

任何时候网络层接收到一份要发送的 IP 数据报文时，它要判断向本地哪个接口发送数据，并查询该接口获得其最大传输单元 MTU。网络层把 MTU 值与要发送的 IP 数据报文长度进行比较，如果 IP 数据报文的长度比 MTU 值大，那么 IP 数据报文就需要进行分片，分片后的数据报文长度小于等于 MTU。

【经验之谈】 MTU 值其实是与数据链路类型有关的，因为不同数据链路中帧封装的“数据”字段（也就是上层数据包的整体大小）是有长度限制的，如以太网的“数据”字段的最大长度是 1 500 个字节，但现在一般都支持超长帧（Jumbo Frame），所以实际上的最大取值不一定等于数据帧中的“数据”字段的最大值。

另外，由于 QoS 队列长度有限，如果 MTU 配置过小，而报文尺寸较大，可能会造

成分片过多，报文被 QoS 队列丢弃；相反，如果 MTU 值配置过大，会造成报文的传输速率较慢，甚至会造成报文丢失。

配置三层以太网接口 MTU 的方法也很简单，就是在对应的以太网接口视图下使用 **mtu** *mtu* 命令配置。参数 *mtu* 用来指定以太网接口的 MTU 值，单位是字节，但不同以太网接口类型和不同 AR G3 系列路由器所支持的具体范围并不完全相同。2FE、4GEW-T 和 4GEW-S 接口卡上的以太网接口取值范围为 46～1 610；主控板和 1GEC 类型接口卡的以太网接口取值范围如下。

① AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2204/2204-S 和 AR2220L：46～1 610。

②AR2220/2220-S/3200、AR2201-48FE/2201-48FE-S/2240/2240-S/2202-48FE：46～9 202。

缺省情况下，以太网接口的 MTU 值为 1 500 字节，可用 **undo mtu** 命令恢复为缺省情况。

注意 使用本命令改变以太网接口最大传输单元 MTU 后，需要在此接口视图下执行 **restart** 命令重启接口，以保证配置的 MTU 生效。如果在同一个以太网接口视图下重复执行本命令，新配置将覆盖旧配置。

2. 配置 Combo 接口工作模式

Combo 接口是一个逻辑接口，一个 Combo 接口对应设备面板上一个 GE 电接口和一个 GE 光接口，而在设备内部只有一个转发接口。电接口与其对应的光接口是光电复用关系，**两者不能同时工作**（例如当激活光接口时，对应的电接口就自动处于禁用状态），用户可根据组网需求选择使用电接口或光接口。电接口和光接口共用一个接口视图。当用户需要激活电接口或光接口、配置电接口或光接口的属性（如速率、双工模式等）时，可在同一接口视图下配置。

可强制配置 Combo 接口为其选择一种工作模式，只需在对应的以太网接口视图下使用 **combo-port** { **copper** | **fiber** }命令配置即可。选择二选一选项 **copper** 时，强制指定 Combo 接口的工作模式为电口模式，即使用网线传输数据；选择二选一选项 **fiber** 时，强制指定 Combo 接口的工作模式为光口模式，即使用光纤传输数据。**但所选择的模式一定要与对端接口的模式一致**，否则会导致与对端接口对接失败。缺省情况下，Combo 接口的工作模式为电口模式，可用 **undo combo-port** 命令恢复为缺省情况。

说明 AR G3 系列路由器的 Combo 接口支持情况如下：

① AR150/150-S/200/200-S 系列不支持 Combo 接口；

② AR160 系列支持 Combo 接口，接口编号为 GE0/0/4；

③ AR1200/1200-S、AR2204/2204-S、AR2220/2220-S、AR2240/2240-S 和 AR3200 系列都支持 1GEC 接口卡提供的 Combo 接口；

④ AR2201-48FE/2201-48FE-S、AR2202-48FE、AR2204/2204-S、AR2220/2220-S 和 AR2220L 主控板上只有一个 Combo 接口，接口编号为 GE0/0/0；

⑤ AR2240/2240-S 和 AR3200 系列主控板上还有两个 Combo 接口，接口编号分别

为 GE0/0/0 和 GE0/0/1，这两个 Combo 接口是独立的，互不干扰。

3.2.7 以太网接口管理

以太网接口的维护工作，包括通过环回功能检测接口转发是否正常、清除接口统计信息这两个方面。下面分别予以介绍。

1. 配置环回检测功能

在进行某些特殊功能测试时，例如初步定位以太网故障时，需要开启以太网接口环回检测功能，以检测当前接口是否与其他接口构成了二层环路。

环回检测可以有两种方式。

① 硬件环回：用硬件将收发端进行短接，使被测设备接收自己发出来的信号。这不是本节所介绍的内容。

② 软件环回：它又分为“远端环回”（外环回）和“本地环回”（内环回）两种。“外环回”指对端向本端发出报文时，本端接收到报文后不按照报文的目的地址进行转发，而是直接将报文再发给对端。“内环回”是指本端发出的报文通过系统内部发回给本端，即接口对内自环。

以太网接口不支持外环回，所以本节介绍的环回检测功能仅指内环回检测。

配置以太网接口内环回检测功能的方法是在对应接口视图，或者一个端口组视图（要为多个接口批量开启内环回检测功能时）下使用 **loopback internal** 命令配置。缺省情况下，以太网接口的环回检测功能处于关闭状态，可用 **undo loopback** 命令取消接口的环回检测功能。

以太网接口开启环回检测功能时将工作在全双工状态，关闭环回检测功能后恢复原有配置。配置环回检测功能会导致设备以太网接口或链路不能正常工作，因此测试完毕后，应及时执行取消环回。

2. 清除统计信息

接口统计信息有助于分析接口的故障原因和接口的工作状态。当你需要统计一定时间内以太网接口的流量信息时，需要在统计开始前清除该接口下原有的统计信息。但要注意，清除统计信息后，以前的统计信息将无法恢复。

① 可执行 **reset counters interface** [*interface-type* [*interface-number*]]用户视图命令清除指定接口的统计信息。

② 执行 **reset counters if-mib interface** [*interface-type* [*interface-number*]] 用户视图命令清除网管的接口流量统计信息。

3.2.8 典型故障分析与排除

在以太网接口配置中，最常见的一个错误就是链路上的两端接口双工模式和速率的自动协商配置不一致，导致接口频繁 Up/Down。

出现这一故障现象后，可以在对应设备上通过执行 **display interface** [*interface-type* [*interface-number*]]命令查看对应接口的双工模式和速率的自动协商配置信息。下面是一个具体的 **display interface** 命令输出示例。

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Switch Port, PVID :      1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
Last physical up time    : 2010-07-21 15:35:37
Last physical down time : 2010-07-20 01:06:25
Current system time: 2010-07-21 16:07:53-05:13
Port Mode: COMMON COPPER
Speed :   100,   Loopback: NONE
Duplex: FULL,   Negotiation: ENABLE
Mdi     : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -
<省略>
```

在这里关键是查看输出信息中的双工模式（**Duplex** 字段）和速率（**Speed** 字段）的配置。这里要确定采用自动协商状态，还是采用非自动协商状态。

① 如果采用的是自动协商状态，则要查看以上输出信息中双工模式和速率中对应的 **Negotiation** 字段。

如果显示的信息是“ENABLE”，则表示接口的双工模式或者速率工作在自动协商状态下；如果显示的信息是“DISABLE”，则表示接口的双工模式或者速率工作在非自动协商状态下。配置时要确保链路两端接口的双工模式或者速率的协商状态一致，要么都工作在自动协商状态下，要么都工作在非自动协商状态下。在接口视图下可以使用 **negotiation auto** 命令调整接口的双工模式或者速率的自动协商状态。如果在自动协商状态下接口仍然频繁 Up/Down，可以尝试将接口改成非自动协商状态，手动强制指定链路两端的接口速率、双工模式一致。

② 如果速率配置为非自动协商状态，出现这种故障现象时，可查看以上输出信息中的 **speed** 字段，如发现链路两端的接口速率不一致，请在对应的接口视图下执行 **speed** 命令调整两接口的速率，使它们一致。

③ 如果双工模式配置为非自动协商状态，出现这种故障现象时，可查看以上输出信息中的 **Duplex** 字段，如发现链路两端的接口双工模式不一致，请在对应的接口视图下执行 **duplex** 命令调整两接口的双工模式，使它们一致。

3.3 Serial 接口配置与管理

Serial 接口是最常用的广域网接口之一，可工作在同步方式或异步方式下，因此通常又被称为同/异步串口。在 AR G3 系列路由器中，Serial 接口由 1SA（1 端口 SA）/2SA（2 端口 SA）接口卡（图 3-5 为 2SA 接口卡）提供，**仅 AR1200 系列、AR1220-S、AR2202-48FE、AR2204/2240-S、AR2220L、AR2220/2220-S、AR2240 和 AR3260 支持配置 Serial 接口。**

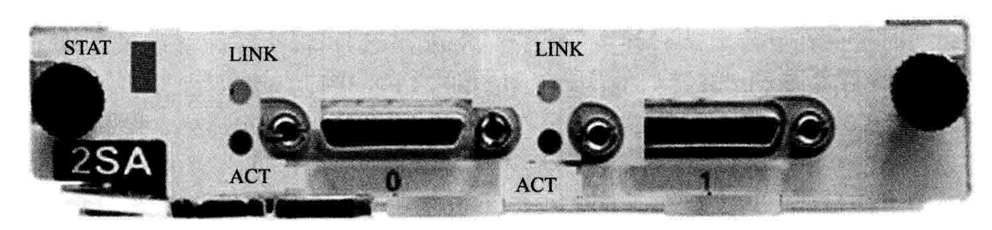


图 3-5　2SA 接口卡

3.3.1　同/异步 Serial 接口

在以上这些支持 Serial 接口的设备中，支持的同步串口是配置为工作在同步方式的同/异步串口，接口名称为 Serial；支持的异步串口有两种。

- 将同/异步串口配置为工作在异步方式，接口名称为 Serial。
- 专用异步串口，接口名称为 Async。

1. Serial 接口工作在同步方式

Serial 接口的缺省工作方式为同步方式。当将 Serial 接口作为 DDN 专线连接，或 Serial 接口对连时工作在同步方式。在同步方式下 Serial 接口具有以下特性。

① Serial 接口可以工作在 DTE（Data Terminal Equipment，数据终端设备）和 DCE（Data Circuit-terminating Equipment，数据电路终端设备）两种方式。

在 Serial 接口插入 DTE 线缆（带针状连接器的一端，俗称"公头"）的设备称为 DTE 设备，用户端的路由器设备；在 Serial 接口插入 DCE 线缆（带孔状连接器的一端，俗称"母头"）的设备称为 DCE 设备，如各种服务器主机，或者运营商的路由器设备。一般情况下，路由器设备作为 DTE 设备，接受 DCE 设备提供的时钟。

在用户私网中，可以根据需要随意指定串行链路的任意一端路由器设备作为 DTE 或者 DCE，DCE 的一端用来指定时钟，DTE 的一端用来与 DCE 时钟同步，**即指定作为 DCE 设备的一端要配置波特率，且在 DTE 设备一端要配置与 DCE 端波特率相等的虚拟波特率**（具体将在本节后面介绍）。金融一体机 AR2202-48FE 主控板上的 Serial 接口仅支持同步方式，仅支持作为 DTE 设备。

② 链路层支持的协议类型包括 PPP、帧中继（FR）和 HDLC。

③ 支持 IP 网络层协议，也就是可以配置 IP 地址。

同步方式下的 Serial 接口主要运用于企业分支机构和总部间通过 PPP 链路实现园区网间的互联，如图 3-6 所示。

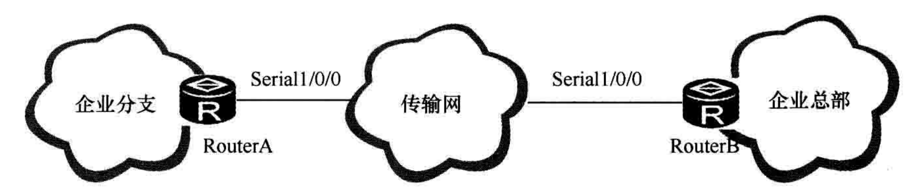


图 3-6　同步方式下 Serial 接口的典型应用场景示意图

2. Serial 接口工作在异步方式

当将 Serial 接口作为异步专线连接，或使用 Serial 接口进行 Modem 拨号、数据备份

和接入终端时工作在异步方式。异步方式下，Serial 接口可以工作在协议模式或流模式。

① 协议模式是指 Serial 接口的物理连接建立之后，接口直接采用已有的链路层协议配置参数，然后建立链路。在协议模式下，链路层协议类型为 PPP，支持 IP 网络层协议。

② 流模式是指 Serial 接口两端的设备进入交互阶段后，链路一端的设备可以向对端设备发送配置信息，设置对端设备的物理层参数，然后建立链路。在流模式下，不支持链路层协议和 IP 网络层协议配置。

3.3.2 配置同步方式下 Serial 接口的物理和链路属性

上节介绍过，Serial 接口在同步工作方式下又有 DTE 和 DCE 两种工作方式。一般情况下，同步串口通常作为 DTE 设备，接受 DCE 设备提供的时钟。但在配置同步方式 Serial 接口之前，需要在设备上成功安装、注册 1SA/2SA 接口卡。

1. 配置工作在 DTE 或 DCE 方式下 Serial 接口的物理属性

同步方式下 Serial 接口（DTE 或 DCE 方式）的物理属性都有缺省值，故一般不用配置，但也可按照表 3-9 所示的配置方法修改属性的取值（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表 3-9 DTE 或 DCE 方式下 Serial 接口的物理属性配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface serial** *interface-number* 例如：[Huawei] **interface serial** 1/0/0	键入要配置物理属性的 DTE 或者 DCE 方式下 Serial 接口，进入接口视图
3	**physical-mode sync** 例如：[Huawei-Serial1/0/0] **physical-mode async**	配置 Serial 接口工作在同步方式，**必须与对端设备的 Serial 接口配置相同的工作方式**。且如果在同一个 Serial 接口视图下重复执行 **physical-mode** 命令且参数不同时，则新配置将覆盖老配置 缺省情况下，Serial 接口工作在同步方式
4	**virtualbaudrate** *baudrate* 例如：[Huawei-Serial1/0/0] **virtualbaudrate** 72000	（二选一可选）配置同步方式下 **DTE 设备** Serial 接口的虚拟波特率。可选的虚拟波特率有：1 200、2 400、4 800、9 600、19 200、38 400、56 000、57 600、64 000、72 000、115 200、128 000、192 000、256 000、384 000、512 000、768 000、1 024 000 和 2 048 000，单位是 bit/s 如果在同一个 Serial 接口视图下重复执行本命令时，新配置将覆盖老配置 缺省情况下，同步方式下 Serial 接口的虚拟波特率为 64 000 bit/s，可用 **undo virtualbaudrate** 命令恢复为缺省情况
	baudrate *baudrate*	（二选一可选）配置同步方式下 **DCE 设备** Serial 接口的波特率，要保证配置的波特率与对端（DTE）配置的虚拟波特率值相同，否则会导致报文被丢弃 同步方式下 Serial 接口的波特率的取值同前面介绍的 Serial 接口的虚拟波特率 缺省情况下，同步方式下 Serial 接口的波特率为 64 000 bit/s，可用 **undo baudrate** 命令恢复为缺省情况

（续表）

步骤	命令	说明
5	**clock** { **rc** | **tc** } 例如：[Huawei-Serial1/0/0] **clock rc**	（可选）配置同步方式下 **DTE 设备** Serial 接口的时钟模式。命令中的选项说明如下 ● **rc**：二选一选项，指定同步方式下 Serial 接口使用接收时钟模式，接收 DCE 设备的时钟 ● **tc**：二选一选项，指定同步方式下 Serial 接口使用自己的内部时钟模式 因为在通信过程中，为保证通信双方能够准确无误地进行数据交换，需要通信双方工作在时钟同步状态，所以通常选择 **rc** 选项，从 DCE 设备接收时钟，以确保链路两端的时钟是完全一致的。如果在同一个 Serial 接口视图下重复执行 **clock** 命令且参数不同时，新配置将覆盖老配置 缺省情况下，同步方式下 Serial 接口的时钟模式为内部时钟（tc）模式，可用 **undo clock** 命令恢复为缺省情况
6	**invert transmit-clock** 例如：[Huawei-Serial1/0/0] **invert transmit-clock**	（可选）配置翻转同步方式下 Serial 接口发送的时钟信号。在某些特殊情况下，时钟在线路上会产生时延，导致两端设备失步或报文被大量丢弃，这时可以将 DTE 侧设备同步串口的发送或接收时钟信号翻转（翻转时钟信号的电平，以产生新的时钟），以消除时延的影响 缺省情况下，不翻转同步方式下 Serial 接口发送的时钟信号，可用 **undo invert transmit-clock** 命令恢复为缺省情况
7	**invert receive-clock** 例如：[Huawei-Serial1/0/0] **invert receive-clock**	（二选一可选）配置翻转同步方式下 Serial 接口的接收时钟信号 缺省情况下，不翻转同步方式下 Serial 接口的接收时钟信号，可用 **undo invert receive-clock** 命令恢复为缺省情况
	invert receive-clock auto 例如：[Huawei-Serial1/0/0] **invert receive-clock** auto	（二选一可选）配置同步方式下 Serial 接口的接收时钟信号的自动翻转功能 缺省情况下，不自动翻转同步方式下 Serial 接口的接收时钟信号，可用 **undo invert receive-clock auto** 命令取消自动翻转功能
8	**detect dsr-dtr** 例如：[Huawei-Serial1/0/0] **detect dsr-dtr**	（可选）使能同步方式下 Serial 接口的 DSR（Data Set Ready，数据装置就绪）和 DTR（Data Terminal Ready，数据终端就绪）信号检测功能，可以用于判断同步方式下 Serial 接口和异步方式下 Serial 接口的状态。DSR 信号用于由 DCE 设备通知 DTE 设备自己是否已经处于工作状态；DTR 信号用于由 DTE 设备通知 DCE 设备自己是否已经处于工作状态 缺省情况下，使能同步方式下 Serial 接口的 DSR 和 DTR 信号检测功能，可用 **undo detect dsr-dtr** 命令去使能 Serial 接口的 DSR 和 DTR 信号检测功能
9	**detect dcd** 例如：[Huawei-Serial1/0/0] **detect dcd**	（可选）使能同步方式下 Serial 接口的 DCD（Data Carrier Detect，数据载波检测）信号检测功能，该功能和同步方式下 Serial 接口的 DSR 和 DTR 信号检测功能配合使用，用于判断同步串口的状态，用于监视通信线路和 DCE 设备的工作状态 **【说明】** 同步方式下 Serial 接口的状态的判断分为以下两种情况

（续表）

步骤	命令	说明
9	**detect dcd** 例如：[Huawei-Serial1/0/0] **detect dcd**	● 如果使能同步方式下 Serial 接口的 DSR 和 DTR 信号检测功能，系统在判断同步方式下 Serial 接口的状态（Up 或 Down）时，缺省情况下将同时检测 DSR 信号、DCD 信号以及接口是否外接电缆。只有当 DSR 信号和 DCD 信号有效且接口外接电缆时，系统才认为同步方式下 Serial 接口处于 Up 状态，否则为 Down 状态 ● 如果不使能同步方式下 Serial 接口的 DSR 和 DTR 信号检测功能，系统在判断同步方式下 Serial 接口的状态（Up 或 Down）时，只要系统检测到外接电缆，就可以判断同步方式下 Serial 接口处于 Up 状态 缺省情况下，已使能同步方式下 Serial 接口的 DCD 信号检测功能，可用 **undo detect dcd** 命令去使能同步方式下 Serial 接口的 DCD 信号检测功能
10	**reverse-rts** 例如：[Huawei-Serial1/0/0] **reverse-rts**	（可选）配置翻转同步方式下 Serial 接口的 RTS（Request To Send，请求发送）信号。这主要用于半双工模式下，因为缺省情况时同步方式下 Serial 接口工作在全双工模式下，为了兼容一些工作在半双工模式的设备，可以使用本命令翻转同步方式下 Serial 接口的 RTS 信号，造成 RTS 信号无效，这样本端接口发送数据时，对端接口不会发送数据 缺省情况下，不翻转同步方式下 Serial 接口的 RTS 信号，可用 **undo reverse-rts** 命令恢复为缺省情况

2. 配置同步方式下 Serial 接口的链路层属性

缺省情况时，同步方式下 Serial 接口（DTE 或 DCE 方式）的链路层属性都有缺省值，故一般也无需配置。但也可按照表 3-10 所示的配置方法修改属性的取值（**注意：其中属性配置没有严格的先后次序**）。

表 3-10　　同步方式下 Serial 接口的链路层属性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface serial** *interface-number* 例如：[Huawei] **interface serial** 1/0/0	键入要配置链路属性的 DTE 或者 DCE 方式下 Serial 接口，进入接口视图
3	**link-protocol ppp** 例如：[Huawei-Serial1/0/0] **link-protocol ppp**	（多选一可选）配置同步方式下 Serial 接口封装 PPP。当接口目前封装的链路层协议不是 PPP，但需要封装成 PPP 时，需要使用此命令 缺省情况下，除以太网接口外，其他接口封装的链路层协议均为 PPP
	link-protocol fr [ietf | nonstandard] 例如：[Huawei-Serial1/0/0:0] **link-protocol fr nonstandard**	（多选一可选）配置同步方式下 Serial 接口封装帧中继协议。命令中的选项说明如下 ● **ietf**：二选一选项，指定帧中继封装格式为 IETF 标准封装格式 ● **nonstandard**：二选一选项，指定帧中继封装格式为非标准兼容封装格式

（续表）

步骤	命令	说明
3	**link-protocol fr** [**ietf** | **nonstandard**] 例如：[Huawei-Serial1/0/0:0] **link-protocol fr nonstandard**	【说明】改变接口的帧中继封装格式后，系统会自动删除该接口下帧中继的所有配置。此时需要重新进行帧中继的相关配置。且执行本命令修改封装格式时，需要先执行 **shutdown** 命令将接口关闭，再执行 **undo shutdown** 命令将接口重启，以保证配置生效。且本命令为覆盖式命令，以最后一次配置为准 当封装帧中继协议时，缺省情况下，帧的封装格式为 IETF，可用 **undo link-protocol fr** 命令恢复接口封装的链路层协议为缺省情况
	link-protocol hdlc 例如：[Huawei-Serial1/0/0] **link-protocol hdlc**	（多选一可选）配置同步方式下 Serial 接口封装 HDLC 协议。接口封装 HDLC 协议时，IP 地址必须与对端接口的 IP 地址在同一网段 缺省情况下，同步方式下 Serial 接口封装的链路层协议为 PPP，可用 **undo link-protocol hdlc** 命令恢复为缺省情况
4	**code** { **nrz** | **nrzi** } 例如：Huawei-Serial1/0/0] **code nrzi**	配置同步方式下 Serial 接口的链路编码格式。命令中的选项说明如下 • **nrz**：二选一选项，指定链路编码格式为 NRZ（Non Return to Zero，非归零）码格式。NRZ 码使用正电平和负电平代表不同的逻辑（1 或 0），信号在一个码元之间不需要返回零电平 • **nrzi** 二选一选项，指定链路编码格式为 NRZI（Non Return to Zero Inverted，非归零翻转）码格式。NRZI 码用电平的翻转代表一个逻辑，电平保持不变代表另外一个逻辑，信号在一个码元间不需要返回零电平。信号电平的翻转可以提供一种同步机制 如果在同一个 Serial 接口视图下重复执行 **code** 命令且参数不同时，新配置将覆盖老配置。但使用同步方式下 Serial 接口通信的**链路两端设备配置的链路编码方式必须相同**，否则收到的数据帧会被解码错误，认为是错误帧而丢弃 缺省情况下，同步方式下 Serial 接口的链路编码格式为 NRZ，可用 **undo code** 命令恢复为缺省情况
5	**crc** { **16** | **32** | **none** } 例如：[Huawei-Serial1/0/0] **crc 32**	（可选）配置同步方式下 Serial 接口的 CRC（Cyclic Redundancy Check，循环冗余校验）校验方式。命令中的选项说明如下 • **16**：多选一选项，指定同步方式下 Serial 接口使用 16 位 CRC 校验方式（即采用 16 位 CRC 校验码） • **32**：多选一选项，指定同步方式下 Serial 接口使用 32 位 CRC 校验方式（即采用 16 位 CRC 校验码） • **none**：多选一选项，指定同步方式下 Serial 接口不进行 CRC 校验 CRC 校验对数据的一致性进行验证，其算法的精度非常高，而 16 位与 32 位校验码长度的区别在于 32 位的校验精度会更高，但是会占用更多的资源。如果在同一个 Serial 接口视图下重复执行 **crc** 命令且参数不同时，新配置将覆盖老配置 缺省情况下，同步方式下 Serial 接口采用 16 位 CRC 校验方式，可用 **undo crc** 命令恢复为缺省情况

（续表）

步骤	命令	说明
6	**idlecode** { **7e** | **ff** } 例如：[Huawei-Serial1/0/0] **idlecode ff**	（可选）配置同步方式下 Serial 接口的线路空闲码类型。由于同步方式下 Serial 接口传输的是电路信号，应该保证持续有数据在线路上传输，然而当线路比较空闲时，就需要使用线路空闲码表示线路的空闲状态。命令中的选项说明如下 ● **7e**：二选一选项，指定同步方式下 Serial 接口的线路空闲码为 0x7e。实际应用中，推荐使用缺省值，即线路的空闲码类型为 0x7e ● **ff**：二选一选项，指定同步方式下 Serial 接口的线路空闲码为 0xff 链路两端 Serial 接口使用的空闲码类型必须一致，否则会导致通信异常。如果在同一个串行接口视图下重复执行 **idlecode** 命令且参数不同时，新配置将覆盖老配置 缺省情况下，同步方式下 Serial 接口的线路空闲码类型为 0x7e，可用 **undo idlecode** 命令恢复为缺省情况
7	**mtu** *mtu* 例如：[Huawei-Serial1/0/0] **mtu** 1200	（可选）配置同步方式下 Serial 接口的最大传输单元 MTU，取值范围为 128～1 500 整数个字节。执行完本命令后，需要依次执行 **shutdown** 和 **undo shutdown** 或 **restart** 命令，重新启动相应的物理接口，使配置生效 缺省情况下，同步方式下 Serial 接口的 MTU 是 1 500 字节，可用 **undo mtu** 命令恢复为缺省情况
8	**rc bypass enable** 例如：[Huawei-Serial1/0/0] **rc bypass enable**	（可选）配置使能同步方式下 Serial 接口接收方向透明传输功能（允许接收不封装 HDLC 协议头的 HDLC 数据帧）。配置本命令后，同步方式下 Serial 接口不产生上述封装操作，直接将报文透明传输至对端设备。但 AR2202-48FE 机型上的 Serial 接口不支持透明传输功能 缺省情况下，同步方式下 Serial 接口未使能接收方向透明传输功能，可用 **undo rc bypass enable** 命令去使能 Serial 接口接收方向透明传输功能
9	**tc bypass enable** 例如：[Huawei-Serial1/0/0] **tc bypass enable**	（可选）配置使能同步方式下 Serial 接口发送方向透明传输功能。通常情况下，同步方式下 Serial 接口发送 HDLC 数据时，设备会为 HDLC 数据包进行封装，以满足 HDLC 帧格式。配置本命令后，同步方式下 Serial 接口不产生上述封装操作，直接将报文透明传输至对端设备。但 AR2202-48FE 上的 Serial 接口不支持透明传输功能 缺省情况下，同步方式下 Serial 接口未使能发送方向透明传输功能，可用 **undo tc bypass enable** 命令去使能 Serial 接口发送方向透明传输功能

3.3.3 配置异步方式下 Serial 接口物理和链路属性

当使用异步方式下 Serial 接口承载上层数据业务时，需要对异步方式下 Serial 接口的工作方式和相关属性进行配置，使异步方式下 Serial 接口物理层和链路层状态为 Up。但在配置异步方式下 Serial 接口之前，需要在设备上成功安装、注册 1SA（1 端口 SA）/2SA（2 端口 SA）接口卡。

1. 配置异步方式下 Serial 接口物理属性

当用户需要通过异步串口登录设备时，需要在设备上配备 SA（同/异步 WAN 接口）

或者 AS（异步 WAN 接口）单板。如果是在 SA 单板上，需要将 SA 单板上的接口模式设置为异步模式；当用户通过异步串口登录设备时，超级终端的物理属性和设备的物理属性要保持一致。

异步方式下 Serial 接口使用的是 TTY（True Type Terminal，实体类型终端）用户界面，其物理属性可按照表 3-11 所示方法进行配置，包括异步串口的传输速率、流控方式、校验位、停止位和数据位（注意：**属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表 3-11　　异步方式下 Serial 接口物理属性配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**user-interface tty** *tty-number* 例如：[Huawei] **user-interface tty** 1 3	进入 TTY 用户界面视图，取值范围为 1～128 的整数，绝对编号 1～128 对应相对编号 TTY 1～TTY 128。当单板注册成功，且串口工作在异步模式时，设备会随机生成 *tty-number*，可以通过 **display user-interface** 命令查看
3	**speed** *speed-value* 例如：[Huawei--ui-tty1-3] **speed** 115200	（可选）设置 TTY 用户界面的传输速率。取值可以为：600、1 200、4 800、9 600、19 200、38 400、57 600 和 115 200，单位为 bit/s 缺省情况下，传输速率为 9 600 bit/s，可用 **undo speed** 命令恢复用户界面的缺省传输速率
4	**flow-control none** 例如：[Huawei-tty1-3] **flow-control none**	（可选）设置 TTY 用户界面流控方式为无流控 因为缺省情况下，流控方式为 None，所以本步其实可以不用配置
5	**parity** { **even** | **none** | **odd** } 例如：[Huawei--ui-tty1-3] **parity odd**	设置 TTY 用户界面的校验位。命令中的选项说明如下 • **even**：多选一选项，指定采用偶校验。采用此种校验方式时，校验位的值是通过确保每个字节中的“1”的位数为偶数计算得出的 • **none**：多选一选项，指定不进行校验，即无校验位 • **odd**：多选一选项，指定采用奇校验。采用此种校验方式时，校验位的值是通过确保每个字节中的“1”的位数为奇数计算得出的 缺省情况下，校验位为 **none**，即不进行校验，可用 **undo parity** 命令恢复 TTY 用户界面的校验方式为缺省的 **none** 方式
6	**stopbits** { **1.5** | **1** | **2** } 例如：[Huawei--ui-tty1-3] **stopbits** 2	设置 TTY 用户界面的停止位。这里的“停止位”是用来间隔不同字符数据的，仅代表时隙长度。命令中的选项说明如下 • **1.5**：多选一选项，指定停止位为 1.5 位，表示停止位占用了 1.5 个时隙位。此时下一步的数据传输模式配置中只能选择 5 位 • **1**：多选一选项，指定停止位为 1 位，表示停止位占用了 1 个时隙位。此时下一步的数据传输模式配置中只能选择 7 位或 8 位 • **2**：多选一选项，指定停止位为 2 位，表示停止位占用了 2 个时隙位。此时下一步的数据传输模式配置中可选择 6 位、7 位或 8 位 缺省情况下，停止位为 1 位。可用 **undo stopbits** 命令恢复 TTY 用户界面停止位为缺省的 1 位，对应数据位数可以是 6、7、8

（续表）

步骤	命令	说明
7	**databits** { **5** | **6** | **7** | **8** } 例如：[Huawei-ui--tty1-3] **databits** 5	设置用于表示数据的位数，也即数据传输模式。四个多选一选项分别代表数据位为 5 位（用 5 位表示数据）、6 位（用 6 位表示数据）、7 位（用 7 位表示数据）、8 位（用 8 位表示数据）。缺省情况下，数据位数为 8 位，可用 **undo databits** 命令恢复数据数位为缺省的 8 位模式

2. 配置异步方式下 Serial 接口的链路属性

缺省情况下，异步方式下 Serial 接口的链路属性都有缺省值。如果需要修改属性值，可按表 3-12 所示步骤进行配置（这些属性也均有缺省配置，根据实际需要配置），**但其中的各属性配置没有严格的先后次序**。

表 3-12　　异步方式下 Serial 接口属性配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface serial** *interface-number* 例如：[Huawei] **interface serial** 1/0/0	键入要配置异步方式属性的 Serial 接口，进入接口视图
3	**physical-mode** async 例如：[Huawei-Serial1/0/0]**physical-mode async**	配置 Serial 接口工作在异步方式 当设备的 Serial 接口配置为同步方式或异步方式时，**其对端设备的 Serial 接口必须配置为相同的方式**，且如果在同一个 Serial 接口视图下重复执行 **physical-mode** 命令且参数不同时，则新配置将覆盖老配置。**但 AR2202-48FE 机型 Serial 接口不支持通过该命令切换到异步方式** 缺省情况下，Serial 接口工作在同步方式
4	**async mode** { flow | protocol } 例如：[Huawei-Serial1/0/0] **async mode flow**	配置异步方式下 Serial 接口的工作模式。命令中的选项说明如下 ● **flow**：二选一选项，指定异步方式下 Serial 接口工作在流模式 ● **protocol**：二选一选项，指定异步方式下 Serial 接口工作在协议模式 如果在同一个 Serial 接口视图下重复执行 **async mode** 命令且参数不同时，则新配置将覆盖老配置 缺省情况下，异步方式下 Serial 接口工作在协议模式，可用 **undo async mode** 命令恢复为缺省情况
5	**detect dsr-dtr** 例如：[Huawei-Serial1/0/0] **detect dsr-dtr**	（可选）使能异步方式下 Serial 接口的 DSR（Data Set Ready，数据装置就绪）和 DTR（Data Terminal Ready，数据终端就绪）信号检测功能，可以用于判断同步方式下 Serial 接口和异步方式下 Serial 接口的状态。DSR 信号用于由 DCE 设备通知 DTE 设备自己是否已经处于工作状态；DTR 信号用于由 DTE 设备通知 DCE 设备自己是否已经处于工作状态 【说明】异步方式下 Serial 接口的状态判断分为以下两种情况

（续表）

步骤	命令	说明
5	**detect dsr-dtr** 例如：[Huawei-Serial1/0/0] **detect dsr-dtr**	• 如果使能异步方式下 Serial 接口的 DSR 和 DTR 信号检测功能，系统将不仅检测异步方式下 Serial 接口是否外接电缆，同时还要检测 DSR 信号，只有当该信号有效时，系统才认为异步方式下 Serial 接口处于 Up 状态，否则，为 Down 状态 • 如果不使能异步方式下 Serial 接口的 DSR 和 DTR 信号检测功能，系统将不检测异步方式下 Serial 接口是否外接电缆，自动向用户报告异步方式下 Serial 接口的状态为 Up 缺省情况下，已使能异步方式下 Serial 接口的 DSR 和 DTR 信号检测功能，可用 **undo detect dsr-dtr** 命令去使能 Serial 接口的 DSR 和 DTR 信号检测功能
6	**phy-mru** *mrusize* 例如：[Huawei-Serial1/0/0] **phy-mru** 1200	（可选）配置异步方式下 Serial 接口的 MRU（Maximum Receive Unit，最大接收单元），取值范围 4～1 700 整个数字节。配置 Serial 接口上的 MRU 值大于等于 MTU 值，可以保证通信双方都有能力接收来自对端的报文。如果在同一个 Serial 接口视图下重复执行 **phy-mru** 命令时，则新配置将覆盖老配置 缺省情况下，异步方式下 Serial 接口的 MRU 为 1 700 字节，可用 **undo phy-mru** 命令恢复为缺省情况
7	**mtu** *mtu* 例如：[Huawei-Serial1/0/0] **mtu** 1200	（可选）配置异步方式下 Serial 接口的最大传输单元 MTU，取值范围为 128～1 500 整数个字节。执行完本命令后，需要依次执行 **shutdown** 和 **undo shutdown** 或 **restart** 命令，重新启动相应的物理接口，使配置生效 缺省情况下，异步方式下 Serial 接口的 MTU 是 1 500 字节，可用 **undo mtu** 命令恢复为缺省情况

3.3.4 Serial 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 Serial 接口。

① **display interface serial** [*interface-number*]：查看 Serial 接口的基本配置信息和统计信息。

② **display interface brief serial** [*interface-number*]：查看 Serial 接口的物理状态、链路协议状态、带宽利用率及错误报文数等简要信息。

③ **display ip interface brief serial** [*interface-number*]：查看 Serial 接口的物理状态和 IP 地址等信息。

3.3.5 同步方式下 Serial 接口连接网络的配置示例

本示例的基本结构如图 3-7 所示，RouterA 和 RouterB 通过 Serial 接口相连。已知 RouterA 侧的接口为 DTE 接口，RouterB 侧的接口为 DCE 接口，用户希望通信两端能够网络互通。

1. 基本配置思路分析

根据 3.3.2 小节介绍的配置方法，可得出本示例的基本配置思路。

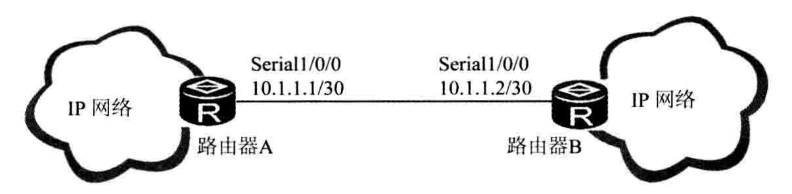


图 3-7 同步方式下 Serial 接口网络连接配置示例基本网络结构

① 配置同步方式下 Serial 接口的物理属性，使接口的物理层状态为 Up。

② 配置同步方式下 Serial 接口的链路层属性，使接口的链路层协议状态为 Up。

③ 配置同步方式下 Serial 接口的 IP 地址，使接口连接的 IP 网络互通。

2. 具体配置步骤

① 配置同步方式下 Serial 接口的物理属性。因为 Serial 接口缺省为同步工作方式，且其物理属性都有对应的缺省值，所以工作方式以及大多数物理属性都可以直接采用对应的缺省值，无需另外配置。在此仅需要在工作在 DTE 方式的 RouterA 的 Serial 接口上配置其时钟模式为使用接收时钟模式，然后可以为两个路由器的 Serial 接口配置比缺省值更高（但必须相等）的波特率（DTE 设备上为虚拟波特率）。

RouterA 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] clock rc   !---配置 DTE 设备上 Serial 接口使用接收时钟模式
[RouterA-Serial1/0/0] virtualbaudrate 72 000    !---配置 DTE 设备上 Serial 接口的虚拟波特率为 72 000 bit/s
```

RouterB 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] baudrate 72 000   !---配置 DCE 设备上 Serial 接口的波特率为 72 000 bit/s，要与 RouterA 上配
置的虚拟波特率相等
```

② 配置同步方式下 Serial 接口的链路层属性。同样由于同步方式下 Serial 接口的链路层属性都有各自对应的缺省值，所以在此也仅需要配置一些希望修改缺省值的属性，如封装的链路层协议（事实上本示例中可不用配置，因为串行链路缺省封装的就是 PPP 协议），MTU 值。在修改了链路层属性后需要依次进行关闭和开启接口，以使配置修改生效。

RouterA 上的配置如下。

```
[RouterA-Serial1/0/0] link-protocol ppp
[RouterA-Serial1/0/0] mtu 1400
[RouterA-Serial1/0/0] shutdown
[RouterA-Serial1/0/0] undo shutdown
```

RouterB 上的配置如下。

```
[RouterB-Serial1/0/0] link-protocol ppp
[RouterB-Serial1/0/0] mtu 1400
[RouterB-Serial1/0/0] shutdown
[RouterB-Serial1/0/0] undo shutdown
```

③ 配置 Serial 接口的 IP 地址。

根据图 3-7 中的两端 Serial 接口的 IP 地址标识配置对应的 IP 地址即可。

RouterA 上的配置如下。

```
[RouterA-Serial1/0/0] ip address 10.1.1.1 30
[RouterA-Serial1/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB-Serial1/0/0] ip address 10.1.1.2 30
[RouterB-Serial1/0/0] quit
```

配置好后，可以通过 **display interface serial** [*interface-number*]命令查看 Serial 接口配置信息和接口工作状态，验证配置结果。

下面仅以 RouterA 上的 Serial 1/0/0 接口为例进行介绍。该 Serial 接口的物理状态和链路层协议状态都是 Up，具体输出信息如下所示。

```
[RouterA] display interface Serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-07-18 11:12:29
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1400, Hold timer is 10(sec)
Internet Address is 10.1.1.1/30
Link layer protocol is PPP
LCP initial
Last physical up time     : 2008-01-09 12:25:52
Last physical down time : 2008-01-09 12:25:51
Current system time: 2008-01-09 19:18:44
Physical layer is synchronous, Virtualbaudrate is 72000 bit/s
Interface is DTE, Cable type is V35, Clock mode is RC
Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
<省略>
```

可以通过 **ping** 命令验证两路由器互联成功。

3.4　CE1/PRI 接口配置与管理

当你需要通过 E1 系统进行业务传输时，可以使用 CE1/PRI 接口。E1 系统和 T1 系统都是 WAN 专线的一种接入线路标准，都属于 PDH（Plesiochronous Digital Hierarchy，准同步数字体系）体系。T1 支持 1.544 Mbit/s 专线电话数据传输，由 24 条独立通道组成，每个通道的传输速率为 64 kbit/s，可同时传输语音和数据。E1 与 T1 类似，支持 2.048 Mbit/s 速率，由 30 路数据信道和两个信令控制信道组成，一共 32 路，每路 64 kbit/s。T1、E1 普遍用于企业专线与因特网进行连接，也可用于因特网服务提供商（ISP）到骨干网的连接。

3.4.1　CE1/PRI 接口简介

CE1/PRI（Channelized E1/Primary Rate Interface，通道化 E1/基群速率接口）是 E1 系统的一种物理接口，可以进行语音、数据和图像信号的传输。CE1/PRI 接口可以工作在 E1 方式（非通道化方式）和 CE1/PRI 方式（通道化方式）。这里要特别注意的是 E1 与 CE1 之间的区别，CE1 是通道化的 E1，也就是把原来整条 2.048 Mbit/s 的 E1 线路分成多个小的传输通道，这样就可以同时承载多个业务流。CE1/RPI 接口常用来接电信

设备。

① 当工作在 E1 方式时，相当于一个不分时隙、数据带宽为 2.048 Mbit/s 的接口，其逻辑特性与同步串口相同，支持 PPP、帧中继等数据链路层协议，支持 IP 网络协议。

② 当工作在 CE1/PRI 方式时，有两种使用方法：CE1 接口和 PRI 接口。在通道化方式下，原来的 2 Mbit/s 的传输线路分成了 32 个 64 kbit/s 的时隙，对应编号为 0～31，其中 0 时隙用于传输同步信息，不能用来传输业务数据。

- 作为 CE1 接口使用时，除 0 时隙外的全部时隙任意分成若干个通道组（channel set），每组时隙捆绑以后，作为一个接口使用，其逻辑特性与同步串口相同，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议。
- 作为 PRI 接口使用时，时隙 16 被作为 D 信道来传输信令，因此，只能从除 0 和 16 时隙以外的时隙中任意选出一组时隙作为 B 信道，将它们同 16 时隙一起，捆绑成一个基群组（pri set），作为一个 ISDN PRI 接口使用，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议。

在 AR G3 系列路由器中，CE1/PRI 接口是由 1E1T1-M 或 2E1T1-M 或 4E1T1-M 或 8E1T1-M 接口卡提供（图 3-8 所示为 1E1T1-M，如 PC 中的串口形状一样），**仅 AR1200 系列、AR1220-S、AR2204、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3200 系列支持配置 CE1/PRI 接口。**

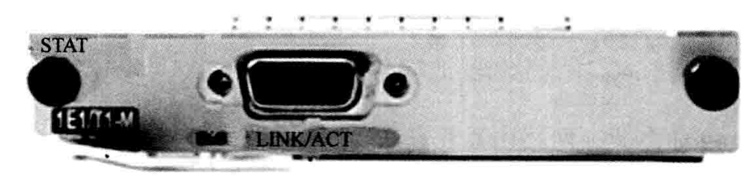


图 3-8 1E1T1-M 接口卡

3.4.2 CE1/PRI 接口物理属性

CE1/PRI 接口物理属性主要包括时钟模式、帧格式、线路空闲码类型、帧间填充符、AIS（Alarm Indication Signal，警告指示信号）和 RAI（Remote Alarm Indication，远程告警指示）。

1. 时钟模式

通信过程中，为保证通信双方能够准确无误地进行数据交换，需要通信双方工作在时钟同步状态。CE1/PRI 接口支持的时钟有主、从两种模式，两个相连接的端口一般为一主一从，时钟由主设备来提供，从设备使用线路上恢复出来时钟，要保证能正确识别接收到的数据。

2. 帧格式

CE1/PRI 接口支持的帧格式有以下两种（**仅工作在 CE1、PRI 方式下的 CE1/PRI 接口支持**）。

① CRC4 帧格式：利用时隙 0 的第一比特形成的复帧，包含 16 个连续的 PCM 帧。

② 非 CRC4 帧格式（基本帧格式）：又称双帧格式或奇偶帧格式，偶数帧时隙 0 传

帧同步信号“0011011”，奇数帧时隙0第二位固定为“1”，以和偶数帧的第二位“0”区别。

CRC4帧格式支持对物理帧进行4比特的循环冗余校验，而非CRC4帧格式不支持。

3. 线路空闲码

“线路空闲码”是指没有被绑定到逻辑通道的时隙上发送的码字。AR G3系列路由器支持两种线路空闲码：0x7e和0xff。

4. 帧间填充符

“帧间填充符”是指已经被绑定到逻辑通道的时隙在没有业务数据发送时发送的码字。AR G3系列路由器支持两种帧间填充符：0x7e和0xff（与支持的线路空闲码一样），并支持对填充符的最少个数进行配置。

5. AIS告警

“AIS告警”又称上游告警，用于指示本端设备接收方向线路有问题或远端设备存在故障。当接收的信号在连续的512 bit里“0”的数量小于3则产生AIS告警；接收的信号在连续的512 bit里“0”的数量不小于3则AIS告警解除。**仅工作在E1方式下的CE1/PRI接口支持。**

6. RAI告警

“RAI告警”是由于设备发现一些问题，如时钟不同步、LOS（Loss of Signal，信号丢失）等导致本地出现帧失步而回发给其上游设备的告警信号。**仅工作在CE1、PRI方式下的CE1/PRI接口支持。**

3.4.3 配置CE1/PRI接口工作在E1方式

当你需要通过带宽为2 M的E1专线接入传输网时，可以配置CE1/PRI接口工作在E1方式。

CE1/PRI接口工作在不同的工作方式时，支持配置的物理属性略有不同。工作在E1方式时，支持配置时钟模式、线路空闲码、帧间填充符和AIS检测，**不支持帧格式和RAI告警配置。**

图3-9所示为CE1/PRI接口工作在E1方式的典型应用场景。企业总部、分支通过传输网（由网络运营商提供）互联，租用带宽为2 Mbit/s的E1专线。

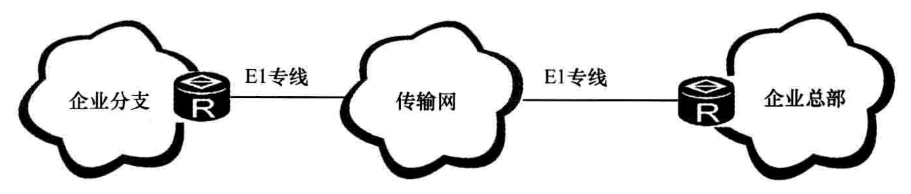


图3-9　CE1/PRI接口工作在E1方式时企业通过E1专线接入传输网的典型结构

配置CE1/PRI接口前，需要确保1E1T1-M或2E1T1-M或4E1T1-M或8E1T1-M接口卡在设备上安装、注册成功。CE1/PRI接口工作在E1方式的具体配置步骤如表3-13所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

注意 除了时钟模式外，CE1/PRI 接口的其他参数必须和对端一致，否则可能导致通信异常。

表 3-13 **CE1/PRI 接口工作在 E1 方式的具体配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1 e1- data** 例如：[Huawei] **set workmode** slot 1 **e1t1 e1-data**	配置 1E1T1-M/2E1T1-M 接口卡工作在 CE1/PRI 模式。命令中的 *slot-id* 参数用来指定需要更改工作模式的接口卡所在的槽位号。可先使用 **display device** 命令查看设备上的接口卡槽位号及类型，再找出单板类型带有"E1/T1-M"的单板槽位号，再使用 **display workmode** { **slot** *slot-id* | **all** }命令查看 1E1T1-M/2E1T1-M 接口卡的工作模式为 e1-data 的槽位号 缺省情况下，1E1T1-M/2E1T1-M 接口卡的工作模式为 e1-data，即 CE1/PRI 模式 【说明】执行该步骤后，需要重启单板并等待一段时间才能使配置生效 4E1T1-M/8E1T1-M 接口卡的工作模式只能为 CE1/PRI，不支持工作模式的切换
3	**controller e1** *interface-number* 例如：[Huawei] **controller e1** 1/0/0	进入指定的 CE1/PRI 接口视图。参数 *interface-number* 用来指定进入的 CE1/PRI 接口的编号
4	在 CE1/PRI 接口视图下，执行 **undo pri-set** 命令取消 pri set 的捆绑 例如：[Huawei-E1 1/0/0] **undo pri-set** 或在 Serial 接口视图，执行 **shutdown** 命令关闭该 Serial 接口 例如：[Huawei]**interface serial** 1/0/0:0 [Huawei-Serial1/0/0:0] **shutdown**	二选一可选 配置取消 pri set 的捆绑（**当你需要从 PRI 方式切换到 E1 方式时，需要执行本步骤，否则不需要执行本步**）
5	**using e1** 例如：[Huawei-E1 1/0/0] **using e1**	配置 CE1/PRI 接口工作在 E1 方式 将 CE1/PRI 的接口工作方式改为 E1 方式后，系统会自动创建一个 Serial 口。Serial 接口的编号是 **serial** *interface-number* **:0**。其中 *interface-number* 是 CE1/PRI 接口的编号，如 **serial** 1/0/0:0。此接口的逻辑特性与同步串口相同，可以视其为同步串口进行进一步的配置，包括 IP 地址、PPP 和帧中继等链路层协议参数、NAT 等 缺省情况下，CE1/PRI 接口的工作方式为 CE1/PRI 方式，可用 **undo using** 命令恢复为缺省工作方式
6	**line-termination** { **75-ohm** | **120-ohm** } 例如：[Huawei-E1 1/0/0] **line-termination 75-ohm**	配置 CE1/PRI 接口所连接的线缆类型。可连接 CE1/PRI 接口的线缆有两种：双绞线和同轴电缆，更换线缆后需要使用本命令设置接口所连接的线缆类型。命令中的选项说明如下 ● **75Ω**：二选一选项，设置 CE1/PRI 接口所连接的线缆是阻抗为 75Ω的非平衡电缆，即同轴电缆

（续表）

步骤	命令	说明
6	**line-termination** { **75-ohm** | **120-ohm** } 例如：[Huawei-E1 1/0/0] **line-termination 75-ohm**	• **120Ω**：二选一选项，设置 CE1/PRI 接口所连接的线缆是阻抗为 120Ω的平衡电缆，即双绞线 缺省情况下，CE1/PRI 接口所连接的线缆是阻抗为 120Ω的平衡电缆，即双绞线，可用 **undo line-termination** 命令恢复为缺省情况
7	**description** *text* 例如: [Huawei-E1 1/0/0] **description** To-[DeviceB]E1-1/0/0	（可选）配置 CE1/PRI 接口描述信息。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小写**，且字符串中不能包含“?”
8	**clock** { **master** | **slave** } 例如：[Huawei-E1 1/0/0] **clock master**	（可选）配置 CE1/PRI 接口的时钟模式。命令中的选项说明如下 • **master**：二选一选项，配置接口使用主时钟模式。当设备作为 DCE 设备使用时，应设置为 **master** 模式，为 DTE 设备提供时钟 • **slave**：二选一选项，配置接口使用从时钟模式。当设备作为 DTE 设备使用时，应设置为 **slave** 模式，从 DCE 设备上获取时钟 当两台路由器的 CT1/PRI 接口直接相连时，必须使两端分别工作在从时钟模式和主时钟模式 缺省情况下，接口使用从时钟模式，可用 **undo clock** 命令恢复为缺省情况
9	**data-coding** { **inverted** | **normal** } 例如：[Huawei-E1 1/0/0] **data-coding inverted**	（可选）配置 CE1/PRI 接口是否对数据进行翻转。数据翻转的原理是将数据码流中的“1”变成“0”，“0”变成“1”，**只有通信双方的 CT1/PRI 接口的数据翻转设置保持一致（都进行翻转或都不进行翻转），才能正常通信**。命令中的选项说明如下 • **inverted**：二选一选项，设置 CT1/PRI 接口对数据进行翻转 • **normal**：二选一选项，设置 CT1/PRI 接口不对数据进行翻转 缺省情况下，不对数据进行翻转，可用 **undo data-coding** 命令恢复为缺省情况
10	**idlecode** { **7e** | **ff** } 例如：[Huawei-E1 1/0/0] **idlecode 7e**	（可选）配置 CE1/PRI 接口的线路空闲码类型。CE1/PRI 接口的线路空闲码类型有两种：0x7e 和 0xff。命令中的选项说明如下 • **7e**：二选一选项，设置 CE1/PRI 接口的线路空闲码为 0x7e • **ff**：二选一选项，设置 CE1/PRI 接口的线路空闲码为 0xff 线路两端的空闲码类型必须一致，否则会导致通信异常 缺省情况下，CE1/PRI 接口的线路空闲码类型为 0x7e，可用 **undo idlecode** 命令恢复为缺省情况，推荐使用缺省值
11	**itf**_{ **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-E1 1/0/0]**itf number** 10 [Huawei-E1 1/0/0] **itf_type ff**	（可选）配置 CE1/PRI 接口帧间填充符的类型和最少个数。命令中的参数和选项说明如下（**注意：这里要分成两个命令来分别配置帧间填充符类型和帧间填充符数，不能用一条命令配置**） • **number** *number*：二选一参数，设置帧间填充符的最少个数，取值范围为 0～14 的整数 • **type**：二选一选项，设置帧间填充符的类型

（续表）

步骤	命令	说明
11	**itf { number** *number* | **type { 7e | ff } }** 例如：[Huawei-E1 1/0/0]**itf number** 10 [Huawei-E1 1/0/0] **itf type ff**	• **7e**：二选一选项，设置帧间填充符类型为 0x7e • **ff**：二选一选项，设置帧间填充符类型为 0xff 缺省情况下，CE1/PRI 接口的帧间填充符类型为 0x7e，最少个数为 4 个，可用 **undo itf { number | type }**命令恢复为缺省情况 【说明】**线路两端的帧间填充符必须配置成相同的码型和最少个数**，否则可能导致通信异常。由于有帧间填充符作为额外开销，CE1/PRI 接口的实际传输速率一般达不到带宽值，为了提高 CE1/PRI 接口实际传输速率，用户可以执行 **itf number** 0 命令将帧间填充符的最小个数设置为 0
12	**crc { 16 | 32 | none }** 例如：[Huawei-E1 1/0/0] **crc 32**	（可选）配置 CE1/PRI 接口的 CRC 校验方式。命令中的选项说明如下 • **16**：多选一选项，指定 CE1/PRI 接口使用 16 位 CRC 校验方式（即采用 16 位 CRC 校验码） • **32**：多选一选项，指定 CE1/PRI 接口使用 32 位 CRC 校验方式（即采用 16 位 CRC 校验码） • **none**：多选一选项，指定 CE1/PRI 接口不进行 CRC 校验 如果在同一个 Serial 接口视图下重复执行 **crc** 命令且参数不同，新配置将覆盖老配置。缺省情况下，CE1/PRI 接口采用 16 位 CRC 校验方式，可用 **undo crc** 命令恢复为缺省情况
13	**undo detect-ais** 例如：[Huawei-E1 1/0/0] **undo detect-ais**	取消对当前 CE1/PRI 接口进行 AIS（Alarm Indication Signal）检测。当 CE1/PRI 接口工作在 E1 方式时，需要配置本命令来取消 AIS 检测 缺省情况下，对接口进行 AIS 检测

3.4.4 配置 CE1/PRI 接口工作在 CE1 方式

当需要使用多个低速率（比如 128 K、256 K）E1 通道传输不同业务时，可以配置 CE1/PRI 接口工作在 CE1 方式。工作在 CE1 方式或下节将要介绍的 PRI 方式的 CE1/PRI 接口，支持配置时钟模式、帧格式、线路空闲码、帧间填充符和 RAI 检测。

CE1/PRI 接口工作在 CE1 方式的典型应用场景如图 3-10 所示。企业总部、分支通过传输网（由网络运营商提供）互联，需要使用多个低速率（比如 128 K、256 K）E1 通道传输不同业务，这时需要将 E1 线路中的时隙捆绑为多个通道，每个通道传输一种业务，比如 2 个时隙用于传输语音、4 个时隙用于传输数据。



图 3-10 CE1/PRI 接口工作在 CE1 方式时企业通过 E1 专线接入传输网的典型结构

在配置 CE1/PRI 接口前，同样需要先在设备上成功安装、注册 1E1T1-M 或 2E1T1-M，或 4E1T1-M 或 8E1T1-M 接口卡。CE1/PRI 接口工作在 CE1 方式的具体配置步骤如表 3-14 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。总体上与表 3-13 中 E1 方式的 CE1/PRI 接口配置差不多，主要区别在于接口的工作方式、时隙捆绑、帧格式和 RAI 检测这 4 个方面。



除了时钟模式外，CE1/PRI 接口的其他参数必须和对端一致，否则可能导致通信异常。

表 3-14　　CE1/PRI 接口工作在 CE1 方式的具体配置步骤

步骤	命令	说明	
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图	
2	**set workmode slot** *slot-id* **e1t1 e1-data** 例如：[Huawei] **set workmode** slot 1 **e1t1 e1-data**	配置 1E1T1-M/2E1T1-M 接口卡工作在 CE1/PRI 模式。具体参见上节表 3-13 中的第 2 步	
3	**controller e1** *interface-number* 例如：[Huawei] **controller e1** 1/0/0	进入指定的 CE1/PRI 接口视图。参数 *interface-number* 用来指定进入的 CE1/PRI 接口的编号	
4	在系统视图下，执行命令 **shutdown** 命令关闭该 Serial 接口 例如：[Huawei]**interface serial** 1/0/0:0 [Huawei-Serial1/0/0:0] **shutdown**	二选一可选	（可选）配置取消 pri set 的捆绑（**当你需要从 PRI 方式切换到 CE1 方式时，需要执行本步骤，否则不需要执行本步**）
	在 CE1/PRI 接口视图下，执行 **undo pri-set** 命令取消 pri set 的捆绑 例如：[Huawei-E1 1/0/0] **undo pri-set**		
5	**using ce1** 例如：[Huawei-E1 1/0/0] **using ce1**	配置 CE1/PRI 接口工作在 CE1 方式。当 CE1/PRI 接口使用 CE1/PRI 工作方式时，2 Mbit/s 的传输线路分成了 32 个 64 kbit/s 的时隙，对应编号为 0～31，其中 0 时隙用于传输同步信息 执行本步骤后，系统会自动创建一个 Serial 口。Serial 接口的编号是 **serial** *interface-number : set-number*。其中 *interface-number* 是 CE1/PRI 接口的编号，*set-number* 是 channel set 的编号。此接口的逻辑特性与同步串口相同，可以视其为同步串口进行进一步的配置，包括：IP 地址、PPP 和帧中继等链路层协议参数、NAT 等 缺省情况下，CE1/PRI 接口的工作方式为 CE1/PRI 方式，可用 **undo using** 命令恢复为缺省工作方式	
6	**channel-set** *set-number* **timeslot-list** *list* 例如：[Huawei-E1 1/0/0] **channel-set** 0 **timeslot-list** 1,10-16,18	将 CE1/PRI 接口的时隙捆绑为 channel set。命令中的参数说明如下 ● *set-number*：指定该接口上时隙捆绑形成的通道编号，取值范围为 0～30 的整数 ● *list*：指定通道要捆绑的时隙列表，取值范围为 1～31 的整数。在指定捆绑的时隙时，可以用 *number* 的形式指定单个时隙，也可以用 *number1-number2* 的形式指定一个范围内的时隙，还可以使用 *number1, number2-number3* 的形式，同时指定多个时隙	

（续表）

步骤	命令	说明
6	**channel-set** *set-number* **timeslot-list** *list* 例如：[Huawei-E1 1/0/0] **channel-set** 0 **timeslot-list** 1,10-16,18	【注意】**在一个 CE1/PRI 接口上同一个时间内只能支持一种时隙捆绑方式**，即本命令不能和 **pri-set** 命令同时使用。一个 CE1 接口最多可以捆绑成 31 个通道，即一个时隙一个通道；最少可以只捆绑一个通道，即 31 个时隙捆绑成一个通道 在指定的 CE1 接口下多次执行本命令就可以实现捆绑多个通道，**但同一个时隙不能同时绑定到多个通道中，且对端 CE1/PRI 接口捆绑的具体时隙需要和本端保持一致，否则，会导致通信异常** 缺省情况下，不捆绑任何通道，可用 **undo channel-set** [*set-number*]命令取消指定的已有捆绑
7	**line-termination** { **75-ohm** | **120-ohm** } 例如：[Huawei-E1 1/0/0] **line-termination 75-ohm**	配置 CE1/PRI 接口所连接的线缆类型。具体参见 3.4.3 小节表 3-13 中的第 6 步
8	**description** *text* 例如：[Huawei-E1 1/0/0] **description** To-[DeviceB]E1-1/0/0	（可选）配置 CE1/PRI 接口描述信息。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小**写，且字符串中不能包含“?”
9	**clock** { **master** | **slave** } 例如：[Huawei-E1 1/0/0] **clock master**	（可选）配置 CE1/PRI 接口的时钟模式。具体参见 3.4.3 节表 3-13 中的第 8 步
10	**frame-format** { **crc4** | **no-crc4** } 例如：[Huawei-E1 1/0/0] **frame-format crc4**	配置 CE1/PRI 接口的帧格式。CE1/PRI 接口作为 CE1 接口使用时，支持 CRC4 和非 CRC4 两种帧格式。**但通信双方的帧格式必须相同，否则会产生 CRC4 告警** ● **crc4**：二选一选项，设置 CE1/PRI 接口的帧格式为 CRC4 帧格式 ● **no-crc4**：二选一选项，设置 CE1/PRI 接口的帧格式为非 CRC4 帧格式 **只有 CE1/PRI 接口工作在 CE1/PRI 方式（即配置了 using ce1 命令），才能执行本命令** 缺省情况下，CE1/PRI 接口的帧格式为非 CRC4 帧格式，可用 **undo frame-format** 命令恢复为缺省情况
11	**data-coding** { **inverted** | **normal** } 例如：[Huawei-E1 1/0/0] **data-coding inverted**	（可选）配置 CE1/PRI 接口是否对数据进行翻转。具体参见 3.4.3 小节表 3-13 中的第 9 步
12	**idlecode** { **7e** | **ff** } 例如：[Huawei-E1 1/0/0] **idlecode 7e**	（可选）配置 CE1/PRI 接口的线路空闲码类型。具体参见 3.4.3 小节表 3-13 中的第 10 步
13	**itf** { **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-E1 1/0/0]**itf number** 10 [Huawei-E1 1/0/0] **itf type ff**	（可选）配置 CE1/PRI 接口帧间填充符类型和最少个数。具体参见 3.4.3 小节表 3-13 中的第 11 步
14	**crc** { **16** | **32** | **none** } 例如：[Huawei-E1 1/0/0] **crc 32**	（可选）配置 CE1/PRI 接口形成的逻辑 Serial 接口的 CRC 校验方式。具体参见 3.4.3 小节表 3-13 中的第 12 步

（续表）

步骤	命令	说明
15	**detect-rai** 例如：[Huawei-E1 1/0/0] **detect-rai**	配置当前 CE1/PRI 接口进行 RAI 检测。当设备发现一些问题，如时钟不同步、LoS（Loss of Signal，信号丢失）等，导致本地出现帧失步时，如果开启了 RAI 告警检测功能，设备将会回发给对端设备 RAI 告警 **只有 CE1/PRI 接口工作在 CE1 或 PRI 方式（即配置了 using** ce1 **命令），才能执行本命令** 缺省情况下，接口进行 RAI 检测，可用 **undo detect-rai** 命令取消 RAI 检测

3.4.5 配置 CE1/PRI 接口工作在 PRI 方式

当你需要使用 ISDN PRI 接口接入 ISDN 网络时，可以配置 CE1/PRI 接口工作在 PRI 方式。

CE1/PRI 接口工作在 PRI 方式的典型应用场景如图 3-11 所示。企业总部、分支通过 ISDN（由网络运营商提供）互联，使用 ISDN PRI 接口接入 ISDN。

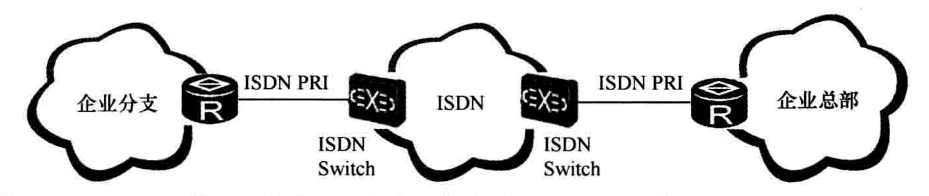


图 3-11 CE1/PRI 接口工作在 PRI 方式时企业通过 ISDN PRI 接口接入 ISDN 的典型结构

在配置 CE1/PRI 接口前，同样需要先在设备上成功安装、注册 1E1T1-M 或 2E1T1-M，或 4E1T1-M 或 8E1T1-M 接口卡。CE1/PRI 接口工作在 PRI 方式的具体配置步骤如表 3-15 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。总体上与 3.4.4 小节 CE1 方式的 CE1/PRI 接口配置差不多，主要区别是 PRI 方式不用取消 pri set 的捆绑，需要将 CE1/PRI 接口的时隙捆绑为 pri set。

注意 CE1/PRI 接口除了时钟模式外的其他参数必须和对端一致，否则可能导致通信异常。

表 3-15 CE1/PRI 接口工作在 PRI 方式的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1 e1-data** 例如：[Huawei] **set workmode** slot 1 **e1t1 e1-data**	配置 1E1T1-M/2E1T1-M 接口卡工作在 CE1/PRI 模式。具体参见 3.4.3 小节表 3-13 中的第 2 步
3	**controller e1** *interface-number* 例如：[Huawei] **controller e1** 1/0/0	进入指定的 CE1/PRI 接口视图。参数 *nterface-number* 用来指定进入的 CE1/PRI 接口的编号
4	**using ce1** 例如：[Huawei-E1 1/0/0] **using ce1**	配置 CE1/PRI 接口工作在 CE1 方式。具体参见 3.4.4 小节表 3-14 中的第 4 步

（续表）

步骤	命令	说明
5	**pri-set** [**timeslot-list** *list*] 例如：[Huawei-E1 1/0/0] **pri-set timeslot-list** 1, 5-8, 16	将 CE1/PRI 接口的时隙捆绑为 pri set，1E1T1-M/2E1T1-M/4E1T1-M/8E1T1-M 接口卡上的 CE1/PRI 接口支持捆绑为一个 pri set。可选参数 **timeslot-list** *list* 用来指定 pri set 中包含的时隙，其取值范围为 1～31 的整数，其中时隙 16 不能被单独捆绑。在指定捆绑的时隙时，可以用 *number* 的形式指定单个时隙，也可以用 *number1-number2* 的形式指定一个范围内的时隙，还可以使用 *number1*, *number2-number3* 的形式，同时指定多个时隙。如果不配置该可选参数，则表示捆绑除 0 时隙外的其他所有时隙，形成一个速率为 30B+D 的 ISDN PRI 接口 【说明】执行本命令后，将自动创建一个 Serial 接口，其逻辑特性与同步串口相同，该 Serial 接口通常被称为 ISDN PRI 接口。ISDN PRI 接口的编号是 **serial** *interface- number*:**15**。其中，*interface-number* 是 CE1/PRI 接口的编号。用户可以在 ISDN PRI 接口上进行进一步配置，包括 DCC 工作参数、PPP 及其验证参数、NAT 等 在一个 CE1/PRI 接口上同一个时间内只能支持一种时隙捆绑方式，即本命令不能和 **channel-set** 命令同时使用。**对端 CE1/PRI 接口捆绑的具体时隙需要和本端保持一致，否则，会导致通信异常** 缺省情况下，CE1/PRI 接口未捆绑成 pri set，可用 **undo pri-set** 命令取消已有的捆绑。但在执行 **undo pri-set** 命令删除 pri set 前，请先执行 **shutdown** 命令将对应的 Serial 接口关闭
6	**line-termination** { **75-ohm** | **120-ohm** } 例如：[Huawei-E1 1/0/0] **line-termination 75-ohm**	配置 CE1/PRI 接口所连接的线缆类型。具体参见 3.4.3 小节表 3-13 中的第 6 步
7	**description** *text* 例如：[Huawei-E1 1/0/0] **description** To-[DeviceB]E1-1/0/0	（可选）配置 CE1/PRI 接口描述信息。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小写**，且字符串中不能包含“?”
8	**clock** { **master** | **slave** } 例如：[Huawei-E1 1/0/0] **clock master**	（可选）配置 CE1/PRI 接口的时钟模式。具体参见 3.4.3 小节表 3-13 中的第 8 步
9	**frame-format** { **crc4** | **no-crc4** } 例如：[Huawei-E1 1/0/0] **frame-format crc4**	（可选）配置 CE1/PRI 接口的帧格式。具体参见 3.4.4 小节表 3-14 中的第 10 步
10	**data-coding** { **inverted** | **normal** } 例如：[Huawei-E1 1/0/0] **data-coding inverted**	（可选）配置 CE1/PRI 接口是否对数据进行翻转。具体参见表 3.4.3 小节表 3-13 中的第 9 步
11	**idlecode** { 7e | ff } 例如：[Huawei-E1 1/0/0] **idlecode 7e**	（可选）配置 CE1/PRI 接口的线路空闲码类型。具体参见 3.4.3 小节表 3-13 中的第 10 步
12	**itf** { **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-E1 1/0/0]**itf number** 10 [Huawei-E1 1/0/0] **itf type ff**	（可选）配置 CE1/PRI 接口帧间填充符类型和最少个数。具体参见 3.4.3 小节表 3-13 中的第 11 步

（续表）

步骤	命令	说明
13	**crc** { **16** | **32** | **none** } 例如：[Huawei-E1 1/0/0] **crc 32**	（可选）配置 CE1/PRI 接口形成的逻辑 Serial 接口的 CRC 校验方式。具体参见 3.4.3 小节表 3-13 中的第 12 步
14	**detect-rai** 例如：[Huawei-E1 1/0/0] **detect-rai**	配置当前 CE1/PRI 接口进行 RAI 检测。具体参见 3.4.4 小节表 3-14 中的第 14 步

3.4.6 CE1/PRI 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果、管理 CE1/PRI 接口，也可用以下用户视图命令清除 CE1/PRI 接口上的统计信息（若你需要统计一定时间内 CE1/PRI 接口生成的串口的流量信息，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display controller e1** *interface-number*：查看对应的 CE1/PRI 接口的状态和参数。

② **display interface serial** *interface-number*：查看对应的 Serial 接口的状态及统计信息。

③ **reset counters interface serial** [*interface-number*]：清除所有或者指定的 CE1/PRI 接口生成的串口上的统计信息。清除接口的统计信息后，所有的统计数据都不能被恢复。

还可为 CE1/PRI 接口配置环回检测功能，方法是在 CE1/PRI 接口视图下使用 **loopback** { **local** | **payload** | **remote** }命令配置。命令中的选项说明如下。

① **local**：多选一选项，设置接口对内自环，指对本设备输出方向环回，用于测试本端设备是否正常。在本端设备上执行命令 **display interface serial** *interface-number*，查看本端设备的 Serial 接口的物理状态（**current state**）是否为 **UP**。如果是 **UP** 状态，则表示本端设备收发报文正常；反之，则表示本端设备收发报文存在故障。

② **payload**：多选一选项，设置接口进行净荷环回，指对本设备输出方向环回有效载荷，通常 TS0（时隙 0）不参与环回。

③ **remote**：多选一选项，设置接口对外环回，指对对端设备发送的输入数据流进行环回，用于测试设备之间链路是否正常。在对端设备上执行命令 **display interface serial** *interface-number*，查看对端设备的 Serial 接口的物理状态（**current state**）是否为 **UP**。如果是 **UP** 状态，则表示设备之间链路正常；反之，则表示设备之间链路存在故障。

注意 进行环回测试将影响系统的性能。测试完毕后，应及时执行命令 **undo loopback** 关闭测试开关。

3.5 E1-F 接口配置与管理

E1-F 接口是 CE1/PRI 接口的简化版本（不能通道化），同样可以进行语音、数据和图像信号的传输。可以利用 E1-F 接口来满足一些简单的 E1 接入需求。

3.5.1 E1-F 接口简介

在 E1 接入应用中，如果不需要划分出多个通道组（channel set）或不需要 ISDN PRI 功能，使用 CE1/PRI 接口就很浪费，此时可以利用 E1-F 接口来满足这些简单的 E1 接入需求。在 AR G3 系列路由器中，E1-F 接口是由 1E1T1-F 或 2E1T1-F 或 4E1T1-F 或 8E1T1-F 接口卡支持（外观与 CE1/PRI 接口卡一样，参见图 3-8），**但也仅有 AR1200 系列、AR1220-S、AR2202-48FE、AR2204/2204-S、AR2220L、AR2220/2220-S、AR2240 和 AR3260 支持配置 E1-F 接口。**

E1-F 接口有两种工作方式：非成帧方式和成帧方式。

① 工作于非成帧方式时，相当于一个不分时隙、数据带宽为 2 048 kbit/s 的接口，其逻辑特性与同步串口（Serial 接口）相同，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议，支持配置时钟模式、线路空闲码、帧间填充符和 AIS 检测等物理属性。

② 工作于成帧方式时，线路分为 32 个时隙，对应编号为 0～31。其中，0 时隙用于传输同步信息，其余时隙可以被任意捆绑成一个通道。E1-F 接口的带宽为 *n* * 64 kbit/s（*n* 是指捆绑的时隙数，最大取值为 31），其逻辑特性也与同步串口相同，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议，支持配置时钟模式、帧格式、线路空闲码、帧间填充符和 RAI 检测等物理属性。

与 CE1/PRI 接口相比，E1-F 接口有如下特点。

① 工作在成帧方式时，E1-F 接口只能将时隙捆绑为一个通道；而 CE1/PRI 接口可以将时隙任意分组，捆绑成多个通道。

② E1-F 接口不支持 PRI 方式。

说明 E1-F 接口支持的物理属性与 CE1/PRI 接口的物理属性是一样的，如时钟模式、帧格式、线路空闲码、帧间填充符、AIS 告警和 RAI 告警，具体参见 3.4.2 小节介绍。

3.5.2 配置 E1-F 接口工作在非成帧方式

当你需要通过带宽为 2 Mbit/s 的 E1 专线接入传输网时，可以配置 E1-F 接口工作在非成帧方式，其典型应用场景如图 3-12 所示。其中企业总部、分支通过传输网（由网络运营商提供）互联，租用带宽为 2 Mbit/s 的 E1 专线。

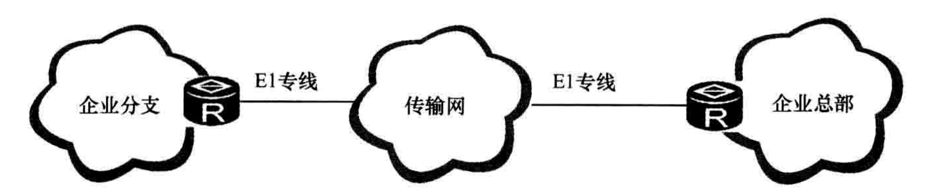
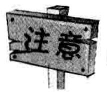


图 3-12 E1-F 接口工作在非成帧方式时企业通过 E1 专线接入传输网的典型结构

配置 E1-F 接口前，需要确保 1E1T1-F 或 2E1T1-F 或 4E1T1-F 或 8E1T1-F 接口卡在设备上安装、注册成功。E1-F 接口工作在非成帧方式的具体配置步骤如表 3-16 所示。总体与 3.4.3 小节介绍的 CE1/PRI 接口工作在 E1 方式下的配置差不多（**注意：其中的属**

性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序）。



E1-F 接口除了时钟模式外的其他参数必须和对端一致，否则可能导致通信异常。

表 3-16　E1-F 接口工作在非成帧方式的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1-f e1-f** 例如：[Huawei] **set workmode slot 1 e1t1-f t1-f**	配置 1E1T1-F/2E1T1-F 接口卡工作在 E1-F 模式。命令中的 *slot-id* 参数用来指定需要更改工作模式的接口卡所在的槽位号。可先使用 **display device** 命令查看设备上的接口卡槽位号及类型，再找出单板类型带有“E1/T1-F”的单板槽位号，再使用 **display workmode**{ **slot** *slot-id* | **all** }命令查看 1E1T1-F/2E1T1-F 接口卡的工作模式为 E1-F 的槽位号 缺省情况下，1E1T1-F/2E1T1-F 接口卡的工作模式为 E1-F 【说明】1E1T1-F/2E1T1-F 接口卡分别实现了一个和两个部分通道化 E1/T1 接口的处理功能，但这块接口卡不能同时提供 E1-F 和 T1-F 接口功能。本命令就是用来设置 1E1T1-F/2E1T1-F 接口卡的工作模式的 执行该命令后，系统将提示用户是否需要重启单板，如果选择“是”，系统自动重启单板。否则用户需要手工执行 **reset slot** 命令使单板重启 4E1T1-F/8E1T1-F 接口卡的工作模式只能为 E1-F，不支持工作模式的切换
3	**interface serial** *interface-number* 例如：[Huawei] **interface serial 1/0/0**	进入指定的 E1-F 接口视图。注意，E1-F 接口使用的是 Searial 接口视图
4	**fe1 unframed** 例如：[Huawei-Serial1/0/0]**fe1 unframed**	将 E1-F 接口的工作方式改为非成帧方式 缺省情况下，E1-F 接口工作在成帧方式，可用 **undo fe1 unframed** 命令恢复为缺省情况
5	**fe1 line-termination** { **75-ohm** | **120-ohm** } 例如：[Huawei-Serial1/0/0]**undo fe1 line-termination 75-ohm**	配置 E1-F 接口所连接的线缆类型。命令中的选项说明具体参见表 3-13 中的第 6 步，只是这里对应的是 E1-F 接口 缺省情况下，E1-F 接口所连接的线缆是阻抗为 120ohm 的平衡电缆，即双绞线，可用 **undo fe1 line-termination** 命令恢复缺省情况
6	**description** *text* 例如：[Huawei-Serial1/0/0] **description** To-[DeviceB]E1-F	（可选）配置 E1-F 接口描述信息。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小写**，且字符串中不能包含“?”
7	**fe1 clock** { **master** | **slave** } 例如：[Huawei-Serial1/0/0]**fe1 clock master**	（可选）配置 E1-F 接口的时钟模式。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 8 步，只是这里对应的是 E1-F 接口 缺省情况下，接口使用从时钟模式，可用 **undo fe1 clock** 命令恢复为缺省情况
8	**fel data-coding** { **inverted** | **normal** } 例如：[Huawei-Serial1/0/0] **fel data-coding inverted**	（可选）配置 E1-F 接口是否对数据进行翻转。命令中的选项说明具体参见 3.4.4 小节表 3-14 中的第 10 步，只是这里对应的是 E1-F 接口 缺省情况下，E1-F 接口不对数据进行翻转，可用 **undo fe1 clock** 命令恢复为缺省情况

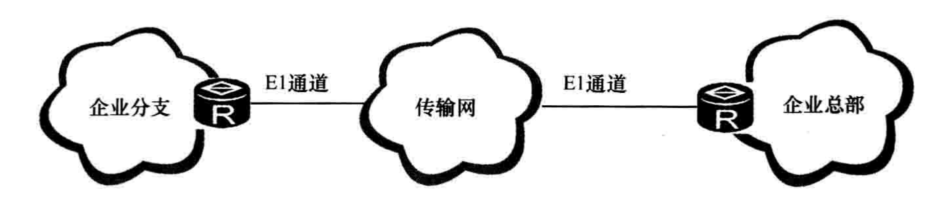
（续表）

步骤	命令	说明
9	**fel idlecode { 7e | ff }** 例如：[Huawei-Serial1/0/0] **fel idlecode 7e**	（可选）配置 E1-F 接口的线路空闲码类型。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 10 步，只是这里对应的是 E1-F 接口
10	**fel itf_{ number** *number* **| type { 7e | ff } }** 例如：[Huawei-Serial1/0/0] **fel itf number** 10 [Huawei-Serial1/0/0] **fel itf_type ff**	（可选）配置 E1-F 接口帧间填充符类型和最少个数。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 11 步，只是这里对应的是 E1-F 接口 缺省情况下，E1-F 接口的线路空闲码为 0x7e，可用 **undo fel idlecode** 命令恢复为缺省情况
11	**undo fel detect-ais** 例如：[Huawei-Serial1/0/0]**undo fel detect-ais**	取消对当前 E1-F 接口进行 AIS 检测。当 E1-F 接口工作在非成帧方式时，需要配置本命令来取消 AIS 检测 缺省情况下，对接口进行 AIS 检测
12	**crc { 16 | 32 | none }** 例如：[Huawei-Serial1/0/0] **crc 32**	（可选）配置 E1-F 接口形成的逻辑 Serial 接口的 CRC 校验方式。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 12 步，只是这里对应的是 E1-F 接口

3.5.3 配置 E1-F 接口工作在成帧方式

若你需要使用一个低速率（比如 512 kbit/s）E1 通道传输业务，可以配置 E1-F 接口工作在成帧方式，其典型应用场景如图 3-13 所示。其中，企业总部、分支通过传输网（由网络运营商提供）互联。当需要使用一个低速率通道传输业务时，需要将 E1 线路中的时隙捆绑为一个通道，然后利用该通道传输业务，比如 8 个时隙用于传输数据。

配置 E1-F 接口前，需要确保 1E1T1-F 或 2E1T1-F 或 4E1T1-F 或 8E1T1-F 接口卡在设备上成功安装、注册。E1-F 接口工作在成帧方式的具体配置步骤如表 3-17 所示。总体配置与上节介绍的 E1-F 接口在非成帧方式（表 3-16）的配置差不多，主要区别就在于工作方式（这里为成帧方式）以及支持配置的帧格式、时隙捆绑和 RAI 检测（**但不再支持非成帧方式下的 AIS 检测**），所以在此仅主要介绍与表 3-16 中不一样的配置。**同样因为属性参数都有缺省配置，故可根据实际需要选择配置。**



E1通道：表示将E1线路时隙任意捆绑形成的通道

图 3-13　E1-F 接口工作在成帧方式时企业通过 E1 专线接入传输网的典型结构

注意 除了时钟模式外，E1-F 接口的其他参数必须和对端一致，否则可能导致通信异常。

表 3-17　E1-F 接口工作在非成帧方式的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1-f e1-f** 例如：[Huawei] **set workmode slot 1 e1t1-f t1-f**	配置 1E1T1-F/2E1T1-F 接口卡工作在 E1-F 模式。具体参见上节表 3-16 中的第 2 步
3	**interface serial** *interface-number* 例如：[Huawei] **interface serial 1/0/0**	进入指定的 E1-F 接口视图
4	**undo fe1 unframed** 例如：[Huawei-Serial1/0/0]**fe1 unframed**	将 E1-F 接口的工作方式改为成帧方式 缺省情况下，E1-F 接口工作在成帧方式
5	**fe1 timeslot-list** *list* 例如：[Huawei-Serial1/0/0] **fe1 timeslot-list** 1-3,8,10	设置 E1-F 接口的时隙捆绑。参数 *list* 用来指定 E1-F 接口捆绑的时隙列表，其取值范围为 1～31 的整数。在指定捆绑的时隙时，可以用 *number* 的形式指定单个时隙，也可以用 *number1-number2* 的形式指定一个范围内的时隙，还可以使用 *number1, number2-number3* 的形式，同时指定多个时隙。当需要改变 E1-F 接口的速率时，需要执行本步骤 缺省情况下，E1-F 接口捆绑除 0 时隙外的其他 31 个时隙，即 E1-F 接口的缺省速率为 1 984 kbit/s，可用 **undo fe1 timeslot-list** 命令恢复为缺省情况
6	**fe1 line-termination** { **75-ohm** | **120-ohm** } 例如：[Huawei-Serial1/0/0]**undo fe1 line-termination 75-ohm**	配置 E1-F 接口所连接的线缆类型。具体参见上节表 3-16 中的第 5 步
7	**description** *text* 例如：[Huawei-Serial1/0/0] **description** To-[DeviceB]E-F	（可选）配置 E1-F 接口描述信息。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小写，**且字符串中不能包含“?”
8	**fe1 frame-format** { **crc4** | **no-crc4** } 例如：[Huawei-Serial1/0/0] **fe1 frame-format crc4**	（可选）设置 E1-F 接口的帧格式。命令中的选项说明具体参见表 3-17 中的第 10 步，只是这里对应的是 E1-F 接口
9	**fe1 clock** { **master** | **slave** } 例如：[Huawei-Serial1/0/0]**fe1 clock master**	（可选）配置 E1-F 接口的时钟模式。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 8 步
10	**fel data-coding** { **inverted** | **normal** } 例如：[Huawei-Serial1/0/0] **fel data-coding inverted**	（可选）配置 E1-F 接口是否对数据进行翻转，命令中的选项说明具体参见 3.4.4 小节表 3-14 中的第 10 步
11	**fel idlecode** { **7e** | **ff** } 例如：[Huawei-Serial1/0/0] **fel idlecode 7e**	（可选）配置 E1-F 接口的线路空闲码类型。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 10 步
12	**fel itf** { **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-Serial1/0/0] **fel itf number** 10 [Huawei-Serial1/0/0] **fel itf type ff**	（可选）配置 E1-F 接口帧间填充符类型和最少个数。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 11 步
13	**fe1 detect-rai** 例如：[Huawei-Serial1/0/0] **fe1 detect-rai**	配置 E1-F 接口进行 RAI 检测。缺省情况下，接口进行 RAI 检测，可用 **undo fe1 detect-rai** 命令取消 RAI 检测
14	**crc** { **16** | **32** | **none** } 例如：[Huawei-Serial1/0/0] **crc 32**	（可选）配置 E1-F 接口形成的逻辑 Serial 接口的 CRC 校验方式。具体参见 3.4.3 小节表 3-13 中的第 12 步

3.5.4 E1-F 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果、管理 E1-F 接口，也可用以下 **reset** 用户视图命令清除 E1-F 接口上的统计信息（若你需要统计一定时间内 E1-F 接口生成的串口的流量信息，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display fe1 serial** *interface-number*：查看指定 E1-F 接口的基本配置信息和告警情况。

② **display interface serial** *interface-number*：查看指定 E1-F 接口的状态及统计信息。

③ **reset counters interface serial** [*interface-number*]：可以清除所有或者指定 E1-F 接口生成的串口上的统计信息。

有关 E1-F 接口的环回检测功能配置方法与 3.4.6 小节介绍的 CE1/PRI 接口的环回检测功能配置方法总体类似，只是这里要在 E1-F 接口视图下配置，并且配置环回检测功能并设置检测方式的命令为 **fe1 loopback** { **local** | **payload** | **remote** }，但对应的选项说明是一样的，参见即可。

3.6 CT1/PRI 接口配置与管理

当你需要通过 T1 系统进行业务传输时，可以使用 CT1/PRI 接口。CT1/PRI 接口是 T1 系统的物理接口，可以用于语音、数据和图像信号的传输。

3.6.1 CT1/PRI 接口简介

T1 系统主要应用于北美和日本（日本采用的 J1，与 T1 基本相似，可以算作 T1 系统），是由 24 个单独的通道组成的，每个通道支持 64 kbit/s 的传输速率，最终可实现 1.544 Mbit/s 的传输速率（比 E1 线路的 2.048 Mbit/s 带宽要窄）。

CT1/PRI 接口是 T1 系统的物理接口，有两种使用方法。

① 当作为 CT1 接口使用时，可以将全部时隙（时隙 1～24）任意地分成若干组，每组时隙捆绑为一个 channel set。每组时隙捆绑后系统自动生成一个接口，其逻辑上等同于同步串口，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议。

② 当作为 PRI 接口使用时，由于编号为 24 的时隙用作 D 信道传输信令，因此只能从除 24 时隙以外的时隙中随意选出一组时隙作为 B 信道，将它们同 24 时隙一起捆绑为一个 pri set，作为一个接口使用，其逻辑特性等同于 ISDN PRI 接口，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议。

AR G3 系列路由器中的 CT1/PRI 接口与 CE1/RPI 接口一样，也是由 1E1T1-M 或 2E1T1-M 接口卡提供（外观参见图 3-8），**但也仅 AR1200 系列、AR1220-S、AR2204、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3260 支持配置 CT1/PRI 接口。**

3.6.2 CT1/PRI 接口物理属性

CT1/PRI 接口物理属性主要包括时钟模式、帧格式、线路空闲码类型、帧间填充符、

AIS 告警和 RAI 告警。与本章前面介绍的 CE1/RPI 接口物理属性总体上类似，**唯一不同的就是所支持的帧格式**（CT1/PRI 接口支持的帧格式为 SF 和 ESF，而 CE1/PRI 接口支持的两种帧格式为 CRC4 和非 CRC4），其他方面参见 3.4.2 节。

① SF（Super Frame，超帧）：由 12 帧组成多帧，共享相同的帧同步信息和信令信息的超帧技术。其中的帧 6 和 12 为两个信令帧。

② ESF（Extended Super Frame，扩展超帧）：由 24 帧组成多帧，共享相同的帧同步信息和信令信息的扩展超帧技术。其中的帧 6、12、18、24 为 4 个信令帧。

3.6.3 配置 CT1/PRI 接口工作在 CT1 方式

当你需要使用多个低速率（比如：128 kbit/s、256 kbit/s）T1 通道传输不同业务时，可以配置 CT1/PRI 接口工作在 CT1 方式。

CT1/PRI 接口工作在 CT1 方式的典型应用场景如图 3-14 所示。企业总部、分支通过传输网（由网络运营商提供）互联，需要使用多个低速率 T1 通道传输不同业务，这时需要将 T1 线路中的时隙捆绑为多个通道，每个通道传输一种业务，比如 2 个时隙用于传输语音、4 个时隙用于传输数据。



图 3-14 CE1/PRI 接口工作在 CT1 方式时企业通过 T1 专线接入传输网的典型结构

在配置 CT1/PRI 接口前，同样需要先在设备上成功安装、注册 1E1T1-M 或 2E1T1-M 接口卡。具体的配置步骤如表 3-18 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

注意 CT1/PRI 接口除了时钟模式外的其他参数必须和对端一致，否则可能导致通信异常。

表 3-18 CT1/PRI 接口工作在 CT1 方式的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1 t1-data** 例如：[Huawei] **set workmode** slot 1 **e1t1 t1-data**	配置 1E1T1-M/2E1T1-M 接口卡工作在 CT1/PRI 模式。命令中的 *slot-id* 参数用来指定需要更改工作模式的接口卡所在的槽位号。可先使用 **display device** 命令查看设备上的接口卡槽位号及类型，再找出单板类型带有“T1/T1-M”的单板槽位号，再使用 **display workmode** { **slot** *slot-id* | **all** }命令查看 1E1T1-M/2E1T1-M 接口卡的工作模式为 t1-data 的槽位号

（续表）

步骤	命令	说明
2	**set workmode slot** *slot-id* **e1t1 t1-data** 例如：[Huawei] **set workmode** slot 1 **e1t1 t1-data**	缺省情况下，1E1T1-M/2E1T1-M 接口卡的工作模式为工作模式为 e1-data，即 CE1/PRI 模式 【说明】执行该步骤后，需要重启单板并等待一段时间才能使配置生效 4E1T1-M/8E1T1-M 接口卡的工作模式只能为 CE1/PRI，不支持工作模式的切换
3	**controller t1** *interface-number* 例如：[Huawei] **controller t1** 1/0/0	进入指定的 CT1/PRI 接口视图。参数 *nterface-number* 用来指定进入的 CT1/PRI 接口的编号
4	在CT1/PRI接口视图下，执行 **undo pri-set** 命令取消 pri set 的捆绑 例如：[Huawei-T1 1/0/0] **undo pri-set**	二选一可选：配置取消 pri set 的捆绑（**当你需要从 PRI 方式切换到 CT1 方式时，需要执行本步骤，否则不需要执行本步**）
	在系统视图下，执行命令 **shutdown** 命令关闭该 Serial 接口 例如：**[Huawei]interface serial** 1/0/0:0 [Huawei-Serial1/0/0:0] **shutdown**	
5	**channel-set** *set-number* **timeslot-list** *list* [**speed** { **56k** | **64k** }] 例如：[Huawei-T1 1/0/0] **channel-set** 0 **timeslot-list** 1,10-16,18	将 CT1/PRI 接口的时隙捆绑为 channel set。命令中的参数和选项说明如下 ● *set-number*：指定该接口上时隙捆绑形成的通道编号，取值范围为 0～23 的整数 ● **timeslot-list** *list*：指定通道捆绑的时隙，其取值范围为 1～24 的整数。在指定捆绑的时隙时，可以用 *number* 的形式指定单个时隙，也可以用 *number1-number2* 的形式指定一个范围内的时隙，还可以使用 *number1, number2-number3* 的形式，同时指定多个时隙 ● **speed** { **56k** | **64k** }：可选项，指定时隙捆绑速率，单位为 kbit/s。选用参数 56 k 时，通道速率为 *N*×56 kbit/s；选用参数 64 k 时，通道速率为 *N*×64 kbit/s。（其中的 *N* 表示通道中捆绑的时隙数量。）系统默认的时隙捆绑速率为 64 kbit/s。但对端配置的时隙捆绑速率必须和本端设备保持一致，否则，会导致通信异常 执行本步骤后，系统会自动创建一个 Serial 口。Serial 接口的编号是 **serial** *interface-number :set-number*。其中 *interface-number* 是 CT1/PRI 接口的编号，*set-number* 是 channel set 的编号。此接口的逻辑特性与同步串口相同，可以视其为同步串口进一步的配置，包括 IP 地址、PPP 和帧中继等链路层协议参数、NAT 等 【注意】在一个 CT1/PRI 接口上同一个时间内只能支持一种时隙捆绑方式，即本命令不能和 **pri-set** 命令同时使用。在指定的 CT1 接口下多次执行本命令就可以实现捆绑多个通道，但同一个时隙不能同时绑定多个通道 缺省情况下，不捆绑任何通道，可用 **undo channel-set** *set-number* 命令取消指定的已有捆绑
6	**description** *text* 例如：[Huawei-T1 1/0/0] **description** To-[DeviceB]T1-1/0/0	（可选）配置接口描述信息。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小写**，且字符串中不能包含“?”

（续表）

步骤	命令	说明
7	**cable { long { -7.5db | -15db | -22.5db } | short { 133ft | 266ft | 399ft | 533ft | 655ft } }** 例如：[uawei-T1 1/0/0] **cable short 133ft**	（可选）配置 CT1/PRI 接口匹配的传输线路的衰减或长度。命令中的选项说明如下 ● **long { −7.5 db | −15 db | −22.5 db }**：二选一选项，配置 CT1/PRI 接口匹配长传输线路时的衰减。匹配 655 英尺以上的传输线路，衰减的选值有−7.5 db、−15 db、−22.5 db，可根据接收端信号质量的不同进行区别选择，当线路质量越差时，信号衰减越大（衰减的绝对值越大） ● **short { 133ft | 266ft | 399ft | 533ft | 655ft }**：二选一选项，配置 CT1/PRI 接口匹配短传输线路时的长度。匹配 655 英尺以下的传输线路，可选参数有 133 ft、266 ft、399 ft、533 ft、655 ft，可根据传输线路的长度，选择相应的长度值 本命令的主要作用是配置发送时的信号波形，以适应不同的传输需要。当接收端收到的信号质量较好时，不需要配置本命令，使用缺省配置即可 缺省情况下，CT1/PRI 接口匹配的传输线路衰减为 long −7.5 db，可用 **undo cable** 命令恢复为缺省情况
8	**clock { master | slave }** 例如：[Huawei-T1 1/0/0] **clock master**	（可选）配置 CT1/TPR 接口的时钟模式。命令中的选项说明如下 ● **master**：二选一选项，配置接口使用主时钟模式。当设备作为 DCE 设备使用时，应设置为 master 模式，为 DTE 设备提供时钟 ● **slave**：二选一选项，配置接口使用从时钟模式。当设备作为 DTE 设备使用时，应设置为 **slave** 模式，从 DCE 设备上获取时钟 当两台路由器的 CT1/PRI 接口直接相连时，**必须使两端分别工作在从时钟模式和主时钟模式**。缺省情况下，接口使用从时钟模式，可用 **undo clock** 命令恢复为缺省情况
9	**alarm-threshold { ais { level-1 | level-2 } | lfa { level-1 | level-2 | level-3 | level-4 } | los { pulse-detection** *value* **| pulse-recovery** *value* **} }** 例如：[Huawei-T1 1/0/0] **alarm-threshold los pulse-detection** 300	（可选）配置 CT1/PRI 接口告警的门限值。命令中的参数和选项说明如下 ● **ais { level-1 | level-2 }**：多选一选项，设置 AIS 告警的门限值。**level-1** 的门限为在一个 SF/ESF 帧内，比特流中的 0 的个数小于等于 2，则 AIS 告警产生；**level-2** 的门限在 SF 格式时为一个 SF 帧内码流 0 的个数小于等于 3，在 ESF 格式时为一个 ESF 帧内码流 0 的个数小于等于 5。缺省情况下，AIS 告警门限值为 level-1 ● **lfa { level-1 | level-2 | level-3 | level-4}**：多选一选项，设置 LFA 告警的门限值。level-1 为 4 个帧同步比特中丢失了 2 个；level-2 为 5 个帧同步比特中丢失了 2 个；leve-3 为 6 个帧同步比特中丢失了 2 个；level-4 仅仅对 ESF 格式有效，在连续 4 个 ESF 帧中出现错误时产生 LFA 告警。缺省情况下，LFA 告警门限值为 level-1 ● **los { pulse-detection** *value* **| pulse-recovery***value* **}**：多选一选项，设置 LOS 告警的门限值。LOS 告警有两个门限值，**pulse-detection** 选项用来配置 LOS 的检测时长门限，参数 *value* 用来指定检测时长门限，取值范围为 16～4 096 的整数，单位为“脉冲周期”；**pulse-recovery**

（续表）

步骤	命令	说明
9	**alarm-threshold** { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection** *value* | **pulse-recovery** *value* } } 例如：[Huawei-T1 1/0/0] **alarm-threshold los pulse-detection** 300	选项用来配置 LOS 的脉冲门限，就是在检测时长内（即 **pulse-detection** 配置的若干个脉冲周期内），检测到的脉冲个数如果小于 **pulse-recovery** 所配置的值，则产生 LOS 告警；脉冲门限的取值范围为 1～256 的整数，单位也为“脉冲周期” 缺省情况下，pulse-detection 参数的值为 176，pulse-recovery 的值为 22，即如果在 176 个脉冲周期内检测到的脉冲数小于 22 个则认为载波丢失，LOS 告警产生，可用 **undo alarm-threshold** { **ais** | **lfa** | **los** { **pulse-detection** | **pulse-recovery** } }命令将告警门限值恢复为以上对应的缺省情况
10	**frame-format** { **esf** | **sf** } 例如：[Huawei-T1 1/0/0] **frame-format sf**	（可选）配置 CT1/PRI 接口的帧格式。命令中的选项说明如下 • **esf**：二选一选项，设置 CT1/PRI 接口的帧格式为扩展超帧 ESF 格式 • **sf**：二选一选项，设置 CT1/PRI 接口的帧格式为超帧 SF 格式 缺省情况下，CT1/PRI 接口的帧格式为 ESF，可用 **undo frame-format** 命令恢复为缺省情况
11	**data-coding** { **inverted** | **normal** } 例如：[Huawei-T1 1/0/0] **data-coding inverted**	（可选）配置 CT1/PRI 接口是否对数据进行翻转。具体参见 3.4.3 小节表 3-13 中的第 9 步
12	**idlecode** { **7e** | **ff** } 例如：[Huawei-T1 1/0/0] **idlecode 7e**	（可选）配置 CT1/PRI 接口的线路空闲码类型。命令的选项说明具体参见 3.4.3 小节表 3-13 中的第 10 步
13	**itf**_{ **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-T1 1/0/0]**itf number** 10 [Huawei-T1 1/0/0] **itf**_**type ff**	（可选）配置 CT1/PRI 接口帧间填充符类型和最少个数。命令的选项说明具体参见 3.4.3 小节表 3-13 中的第 11 步
14	**crc** { **16** | **32** | **none** } 例如：[Huawei-T1 1/0/0] **crc 32**	（可选）配置 CT1/PRI 接口形成的逻辑 Serial 接口的 CRC 校验方式。命令的选项说明具体参见 3.4.3 小节表 3-13 中的第 12 步
15	**detect-rai** 例如：[Huawei-T1 1/0/0] **detect-rai**	配置当前 CT1/PRI 接口进行 RAI 检测。具体参见 3.4.4 小节表 3-14 中的第 15 步

3.6.4 配置 CT1/PRI 接口工作在 PRI 方式

当你需要使用 ISDN PRI 接口接入 ISDN 网络时，可以配置 CT1/PRI 接口工作在 PRI 方式。CT1/PRI 接口工作在 PRI 方式的典型应用场景如图 3-15 所示。企业总部、分支通过 ISDN（由网络运营商提供）互联，使用 ISDN PRI 接口接入 ISDN。

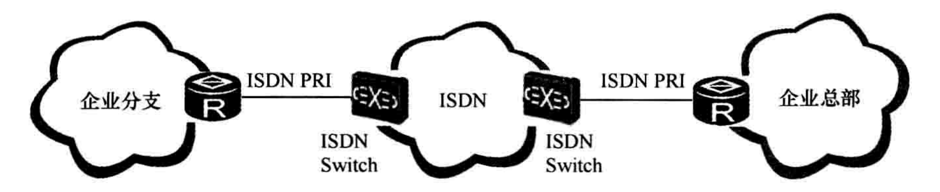


图 3-15　CT1/PRI 接口工作在 PRI 方式时企业通过 ISDN PRI 接口接入 ISDN 的典型结构

在配置CT1/PRI接口前，同样需要先在设备上成功安装、注册1E1T1-M或2E1T1-M接口卡。CT1/PRI接口工作在PRI方式的具体配置步骤如表3-19所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。总体上与3.6.3节CT1方式下的CT1/PRI接口配置差不多，主要区别是PRI方式不用取消pri set的捆绑，需要将CT1/PRI接口的时隙捆绑为pri set，而不是捆绑为一个channel set。

注意 除了时钟模式外，CT1/PRI接口的其他参数必须和对端一致，否则可能导致通信异常。

表3-19　　　　CT1/PRI接口工作在RPI方式的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1 t1-data** 例如：[Huawei] **set workmode** slot 1 **e1t1 t1-data**	配置1E1T1-M/2E1T1-M接口卡工作在CT1/PRI模式。具体参见上节表3-18中的第2步
3	**controller t1** *interface-number* 例如：[Huawei] **controller t1** 1/0/0	进入指定的CT1/PRI接口视图。参数 *nterface-number* 用来指定进入的CT1/PRI接口的编号
4	**pri-set** [**timeslot-list** *list*] 例如：[Huawei-T1 1/0/0] **pri-set timeslot-list** 1, 5-8, 2	将CT1/PRI接口捆绑为一个pri set。命令中的可选参数timeslot-list *list* 用来指定pri set中包含的时隙，其取值范围为1～24的整数，其中时隙24作为D信道使用，不能被单独捆绑。在指定捆绑的时隙时，可用 *number* 的形式指定单个时隙，也可用 *number1-number2* 的形式指定一个范围内的时隙，还可以使用 *number1,number2-number3* 的形式，同时指定多个时隙。如果不配置该参数，则表示捆绑所有时隙形成一个速率为23B+D的ISDN PRI接口 执行 **pri-set** 命令后，将自动创建一个Serial接口，其逻辑特性与ISDN PRI接口相同。Serial接口的编号是“serial *interface-number*:23”。其中，*interface-number* 是CT1/PRI接口的编号 【注意】在一个CT1/PRI接口上同一个时间内只能支持一种时隙捆绑方式，即本命令不能和 **channel-set** 命令同时使用。**对端CT1/PRI接口捆绑的具体时隙需要和本端保持一致，否则会导致通信异常** 缺省情况下，CT1/PRI接口未捆绑成pri set，可用 **undo pri-set** 命令取消已有的捆绑。但在执行 **undo pri-set** 命令删除pri set前，请先执行命令 **shutdown** 将对应的Serial接口关闭
5	**description** *text* 例如：[Huawei-T1 1/0/0] **description** To-[DeviceB]T1-1/0/0	（可选）配置接口描述信息。参数 *text* 用来指定接口的描述信息，1～242个字符，**支持空格，区分大小写**，且字符串中不能包含“?”
6	**cable** { **long** { **−7.5db** | **−15db** | **−22.5db** } | **short** { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** } } 例如：[uawei-T1 1/0/0] **cable short 133ft**	（可选）配置CT1/PRI接口匹配的传输线路的衰减或长度。命令中的选项说明具体参见3.6.3小节表3-18中的第7步

（续表）

步骤	命令	说明
7	**clock** { **master** | **slave** } 例如：[Huawei-T1 1/0/0] **clock master**	（可选）配置 CT1/TPR 接口的时钟模式。具体参见 3.6.3 小节表 3-18 中的第 8 步
8	**alarm-threshold** { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection** *value* | **pulse-recovery** *value* } } 例如：[Huawei-T1 1/0/0] **alarm-threshold los pulse- detection** 300	（可选）配置 CT1/PRI 接口告警的门限值。命令中的选项说明具体参见 3.6.3 小节表 3-18 中的第 9 步
9	**frame-format** { **esf** | **sf** } 例如：[Huawei-T1 1/0/0] **frame-format sf**	（可选）配置 CT1/PRI 接口的帧格式。命令中的选项说明具体参见 3.6.3 小节表 3-18 中的第 10 步
10	**data-coding** { **inverted** | **normal** } 例如：[Huawei-T1 1/0/0] **data- coding inverted**	（可选）配置 CT1/PRI 接口是否对数据进行翻转。命令中的选项说明具体参见 3.4.3 小节表 3-16 中的第 9 步
11	**idlecode** { **7e** | **ff** } 例如：[Huawei-T1 1/0/0] **idlecode 7e**	（可选）配置 CT1/PRI 接口的线路空闲码类型。命令中的选项说明具体参见 3.4.3 小节表 3-16 中的第 10 步
12	**itf** { **number** *number* | type { **7e** | **ff** } } 例如：[Huawei-T1 1/0/0]**itf number** 10 [Huawei-T1 1/0/0] **itf type ff**	（可选）配置 CT1/PRI 接口帧间填充符类型和最少个数。命令中的选项说明具体参见 3.4.3 小节表 3-16 中的第 11 步
13	**crc** { **16** | **32** | **none** } 例如：[Huawei-T1 1/0/0] **crc 32**	（可选）配置 CT1/PRI 接口形成的逻辑 Serial 接口的 CRC 校验方式。命令中的选项说明具体参见 3.4.3 小节表 3-13 中的第 12 步
14	**detect-rai** 例如：[Huawei-T1 1/0/0] **detect-rai**	配置当前 CT1/PRI 接口进行 RAI 检测。具体参见 3.4.4 小节表 3-14 中的第 15 步

3.6.5 CT1/PRI 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果、管理 CT1/PRI 接口，也可用以下 **reset** 用户视图命令清除 CT1/PRI 接口上的统计信息（当你需要统计一定时间内 CT1/PRI 接口生成的串口的流量信息时，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display controller t1** *interface-number*：查看指定 CT1/PRI 接口的状态和参数。

② **display interface serial** *interface-number*：查看指定 Serial 接口的状态及统计信息。

③ **reset counters interface serial** [*interface-number*]：清除所有或者指定 CT1/PRI 接口生成的串口上的统计信息。

有关 CT1/PRI 接口的环回检测功能配置方法与 3.4.6 小节介绍的 CE1/PRI 接口的环回检测功能配置方法完全相同（只是这里要在 CT1/PRI 接口视图下配置），参见即可。

3.7 T1-F 接口配置与管理

与 CE1/PRI 接口有对应的简化版本 E1-F 接口一样，CT1/PRI 也有对应的简化版

本——T1-F 接口（不能通道化）。T1-F 接口可进行语音、数据和图像信号的传输，可以用来满足一些简单的 T1 接入需求。

3.7.1　T1-F 接口简介

在 T1 接入应用中，如果不需要划分出多个通道组（channel set）或不需要 ISDN PRI 功能，使用 CT1/PRI 接口就显得浪费，此时可以利用 T1-F 接口来满足这些简单的 T1 接入需求。

在 AR G3 系列路由器中，与 E1-F 接口一样，T1-F 接口由 1E1T1-F 或 2E1T1-F 接口卡提供，**但也仅有 AR1200 系列、AR2202-48FE、AR1220-S、AR2204、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3260 支持配置 T1-F 接口。**

T1-F 接口只能工作在成帧工作方式。在成帧方式下，可以将 T1-F 接口的全部时隙（时隙 1～24）任意地捆绑成一个组（channel set）。T1-F 接口的带宽为 n×64 kbit/s 或 n×56 kbit/s（n 是指捆绑的时隙数），其逻辑上等同于同步串口，支持 PPP、HDLC 和 FR 数据链路层协议，支持 IP 网络协议。与 CT1/PRI 接口相比，T1-F 接口有如下特点。

① 工作在成帧方式时，**T1-F 接口只能将时隙捆绑为一个通道**；而 CT1/PRI 接口可以将时隙任意分组，捆绑出多个通道。

② T1-F 接口不支持 PRI 方式。

T1-F 接口与 CT1/PRI 接口支持相同的物理属性，包括时钟模式、帧格式、线路空闲码、帧间填充符、RAI 告警，具体参见 3.4.2 小节介绍。

3.7.2　配置 T1-F 接口

当你需要使用一个低速率（比如 512 kbit/s）T1 通道传输业务时，可以配置 T1-F 接口。T1-F 接口的典型应用场景如图 3-16 所示。企业总部、分支通过传输网（由网络运营商提供）互联，需要使用一个低速率通道传输业务，这时需要将 T1 线路中的部分或全部时隙捆绑为一个通道，进行业务数据传输。

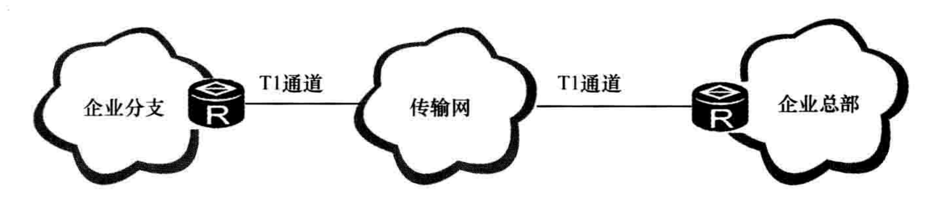


图 3-16　T1-F 接口通过 T1 通道接入传输网的典型结构

在配置 T1-F 接口前，同样需要先在设备上成功安装、注册 1E1T1-F 或 2E1T1-F 接口卡（与 E1-F 接口使用的是相同的接口卡）。T1-F 接口的具体配置步骤如表 3-20 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。其中多数配置与工作在 3.6.3 小节表 3-18 中的 CT1 方式下 CT1/PRI 接口配置类似。

注意　除了时钟模式外，T1-F 接口的其他参数必须和对端一致，否则可能导致通信异常。

表 3-20　T1-F 接口的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**set workmode slot** *slot-id* **e1t1-f e1-f** 例如：[Huawei] **set workmode slot 1 e1t1-f t1-f**	配置 1E1T1-F/2E1T1-F 接口卡工作在 E1-F 模式。命令中的 *slot-id* 参数用来指定需要更改工作模式的接口卡所在的槽位号。可先使用 **display device** 命令查看设备上的接口卡槽位号及类型，再找出单板类型带有“E1/T1-F”的单板槽位号，再使用 **display workmode**{ **slot** *slot-id* | **all** } 命令查看 1E1T1-F/2E1T1-F 接口卡的工作模式为 T1-F 的槽位号 执行该命令后，系统将提示用户是否需要重启单板，如果选择“是”，系统自动重启单板。否则用户需要手工执行 reset slot 命令使单板重启 缺省情况下，1E1T1-F/2E1T1-F 接口卡的工作模式为 E1-F 【说明】1E1T1-F/2E1T1-F 接口卡分别实现了 1 个和 2 个部分通道化 E1/T1 接口的处理功能，**但这块接口卡不能同时提供 E1-F 和 T1-F 接口功能** 4E1T1-F/8E1T1-F 接口卡的工作模式只能为 E1-F，不支持工作模式的切换
3	**interface serial** *interface-number* 例如：[Huawei] **interface serial 1/0/0**	进入指定的 T1-F 接口视图
4	**ft1 timeslot-list** *list* [**speed** { **56k** | **64k** }] 例如：[Huawei-Serial1/0/0] **ft1 timeslot-list** 1-3,8,10	配置 T1-F 接口捆绑时隙和速率。命令中的参数和选项说明如下 ● *list*：指定 T1-F 接口要捆绑的时隙列表，取值范围为 1～24 的整数。在指定捆绑的时隙时，可以用 *number* 的形式指定单个时隙，也可以用 *number1-number2* 的形式指定一个范围内的时隙，还可以使用 *number1, number2-number3* 的形式，同时指定多个时隙 ● **speed** {**56k** | **64k** }：指定时隙捆绑速率，单位为 kbit/s。选择 56 k 选项时，通道速率为 *n*×56 kbit/s；选择 64 k 选项时，通道速率为 *n*×64 kbit/s（其中的 *n* 表示通道中捆绑的时隙数量）。系统默认的时隙捆绑速率为 64 kbit/s 缺省情况下，T1-F 接口对所有时隙进行捆绑，即 T1-F 接口的缺省速率为 1 536 kbit/s（时隙的缺省速率为 64 kbit/s），可用 **undo ft1 timeslot-list** 命令恢复为缺省情况
5	**description** *text* 例如：[Huawei-Serial1/0/0] **description** To-[DeviceB]T1-F	（可选）配置 E1-F 接口描述信息..。参数 *text* 用来指定接口的描述信息，1～242 个字符，**支持空格，区分大小写**，且字符串中不能包含“?”
6	**ft1 cable** { **long** { **-7.5db** | **-15db** | **-22.5db** } | **short** { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** } } 例如：[Huawei-Serial1/0/0] **ft1 cable short** 133ft	（可选）配置 T1-F 接口匹配的传输线路的衰减或长度。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 7 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，T1-F 接口匹配的传输线路衰减为 long −7.5db，可用 **undo ft1 cable** 命令恢复为缺省情况
7	**ft1 clock** { **master** | **slave** } 例如：[Huawei-Serial1/0/0] **ft1 clock master**	（可选）配置 T1-F 接口的时钟模式。命令中的选项具体说明参见 3.6.3 小节的表 3-18 第 8 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，接口使用从时钟模式，可用 **undo ft1 clock** 命令恢复为缺省情况

（续表）

步骤	命令	说明
8	**ft1 alarm-threshold** { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection***value* | **pulse-recovery** *value* } } 例如：[Huawei-Serial1/0/0] **ft1 alarm-threshold los pulse-detection** 300	（可选）配置 T1-F 接口的告警门限。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 9 步，不同的只是这里对应的是 T1-F 接口 缺省情况下：对于 AIS 告警，缺省值为 level-1；对于 LFA 告警，缺省值为 level-1；对于 LOS 告警，pulse-detection 参数的值为 176，pulse-recovery 的值为 22，即默认的情况下，如果在 176 个脉冲周期内检测到的脉冲数小于 22 个则认为载波丢失，LOS 告警产生。可用 **undo ft1 alarm-threshold** { **ais** | **lfa** | **los** { **pulse-detection** | **pulse-recovery** } 命令将对应的类型告警门限值恢复为缺省情况
9	**frame-format** { **esf** | **sf** } 例如：[Huawei-Serial1/0/0]**frame-format sf**	（可选）配置 T1-F 接口的帧格式。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 10 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，T1-F 接口的帧格式为 ESF，可用 **undo ft1 frame-format** 命令恢复为缺省情况
10	**ftl data-coding** { **inverted** | **normal** } 例如：[Huawei-Serial1/0/0] **ftl data-coding inverted**	（可选）配置 T1-F 接口是否对数据进行翻转。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 11 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，T1-F 接口不对数据进行翻转，可用 **undo ft1 data-coding** 命令恢复为缺省情况
11	**ftl idlecode** { **7e** | **ff** } 例如：[Huawei-Serial1/0/0] **ftl idlecode 7e**	（可选）配置 E1-F 接口的线路空闲码类型。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 12 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，T1-F 接口的线路空闲码为 0x7e，可用 **undo ft1 idlecode** 命令恢复为缺省情况
12	**ftl itf** { **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-Serial1/0/0] **ftl itf number** 10 [Huawei-Serial1/0/0] **ftl itf type ff**	（可选）配置 E1-F 接口帧间填充符类型和最少个数。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 13 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，T1-F 接口的帧间填充符类型为 0x7e，最少个数为 4 个，可用 **undo ft1 itf** { **number** | **type** }命令恢复为缺省情况
13	**crc** { **16** | **32** | **none** } 例如：[Huawei-Serial1/0/0] **crc 32**	（可选）配置 E1-F 接口形成的逻辑 Serial 接口的 CRC 校验方式。命令中的选项具体说明参见 3.6.3 小节表 3-18 的第 14 步，不同的只是这里对应的是 T1-F 接口
14	**ft1 detect-rai** 例如：[Huawei-Serial1/0/0]**undo ftl detect-ais**	配置当前 T1-F 接口进行 RAI 检测。具体说明参见 3.6.3 小节表 3-18 的第 15 步，不同的只是这里对应的是 T1-F 接口 缺省情况下，接口进行 RAI 检测，可用 **undo ft1 detect-rai** 命令取消 RAI 检测

3.7.3 T1-F 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 T1-F 接口，也可用以下 **reset** 用户视图命令清除 T1-F 接口上的统计信息（当你需要统计一定时间内 T1-F 接口生成的串口的流量信息时，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display ft1 serial** *interface-number*：查看 T1-F 接口的基本配置信息和告警情况。

② **display interface serial** *interface-number*：查看 T1-F 接口的状态及统计信息。

③ **reset counters interface serial** [*interface-number*]：清除 T1-F 接口生成的串口上的统计信息。

有关 T1-F 接口的环回检测功能配置方法与 3.4.6 小节介绍的 CE1/PRI 接口的环回检测功能配置方法总体一样，只是这里要在 T1-F 接口视图下配置，并且配置环回检测功能并设置检测方式的命令为 **ft1 loopback** { **local** | **payload** | **remote** }，但对应的选项说明是一样的，参见即可。

3.8 3G Cellular 接口配置与管理

当需要通过 3G 网络传输语音、视频等数据业务时，就需要配置 3G Cellular 接口。3G Cellular 接口是设备提供的支持 3G 技术的物理接口，为用户提供了企业级的无线广域网接入服务。

3.8.1 3G Cellular 接口简介

有线广域接入服务（比如光纤、xDSL 或 E1/T1）虽然技术成熟，应用广泛，但是在某些特殊场合下会遇到瓶颈，这些特殊场合包括以下几种。

① 在某些区域比如企业的偏远分支或海上油田，有线广域接入服务不可用或成本太高。

② 某些情形比如灾区现场，需要进行快速连接和临时连接。

③ 某些业务比如加油站、ATM 机，站点分布广泛，有线广域接入服务无法完全覆盖。

④ 企业人员需要进行移动办公。

对于这些特殊场合，企业需要无线广域接入服务来满足业务需求。第三代移动通信 3G（3rd Generation Mobile Telecommunications）能够传输无线广域的语音、视频等数据业务，可以满足企业所需的无线广域接入服务。设备上的 3G Cellular 接口支持 3G 技术，通过配置 3G Cellular 接口作为备份链路或主链路接入 Internet，用户可以利用 3G 网络传输语音、视频等数据业务。

1. 3G Cellular 接口的类型

3G Cellular 接口对 3G Modem 进行管理，在物理层使用 3G Modem 进行无线传输，数据链路层使用 PPP，网络层使用 IP 协议。

AR G3 系列路由器包括如下类型 3G Cellular 接口。

① 对于 AR1200/1200-S 系列、AR2204/2204-S、AR2220L、AR2220/2220-S、AR2240/2240-S 或 AR3200 系列，3G Cellular 接口可以由外置 3G Modem 的 USB 接口（**支持 WCDMA 网络和 CDMA2000 网络**）或内置 3G Modem 的 3G-HSPA+7 接口卡（**仅支持 WCDMA 网络**）提供。

② 对于 AR2201-48FE/2201-48FE-S 和 AR2202-48FE，3G Cellular 接口可以由外置

3G Modem 的 USB 接口提供（支持 WCDMA 网络或 CDMA2000 网络）。

③ 对于 AR150/150-S/160/200/200-S 系列，3G Cellular 接口可以由外置 3G Modem 的 USB 接口提供（**支持 WCDMA 网络或 CDMA2000 网络**）。其中，AR151G-HSPA+7、AR157G-HSPA+7 和 AR207G-HSPA+7 本身也支持 3G Cellular 接口（仅支持 WCDMA 网络），当你购买上述几款设备时，可以根据需要灵活选择不同类型的 3G Cellular 接口。

- 当你选择使用 AR151G-HSPA+7、AR157G-HSPA+7 或 AR207G-HSPA+7 本身提供的 3G Cellular 接口时，其接口编号为 Cellular 0/0/0。
- 当你选择使用外置 3G Modem 的 USB 接口提供的 3G Cellular 接口时，其接口编号为 Cellular 0/0/1。

3G Cellular 接口可以作为主链路或备份链路接入 Internet。无论作为主链路还是备份链路，3G Cellular 接口都需要通过轮询 DCC（拨号控制中心，具体配置将在下章介绍）进行拨号。

2. 可使用的 3G 数据卡

目前使用 AR G3 系列路由器的用户可以选用的 3 G 数据卡中支持 WCDMA 3G 标准的有 E367、E352u、E173u、E180、K4605、K3765、E177、E372，支持 CDMA2000 3G 标准的有 EC1261。华为设备使用的 3 G 数据卡必须为这些 3 G 数据卡，否则可能会出现各种配置问题。

由于不同国家频率规划不一样，不同运营商被授权经营的频段也不一样，因此企业使用 3 G 数据卡满足 3 G 业务时，需要确保运营商提供服务的频段与 3G 数据卡支持频段是一致的。

3. 3G Cellular 接口的应用场景

在 AR G3 系列路由器中，3G Cellular 接口的主要应用体现在以下三个方面。

（1）3G Cellular 接口作为主链路接入 Internet

如图 3-17 所示，AR G3 系列路由器是企业的出口网关，企业采取 3G Cellular 接口作为主链路上行接入 Internet。

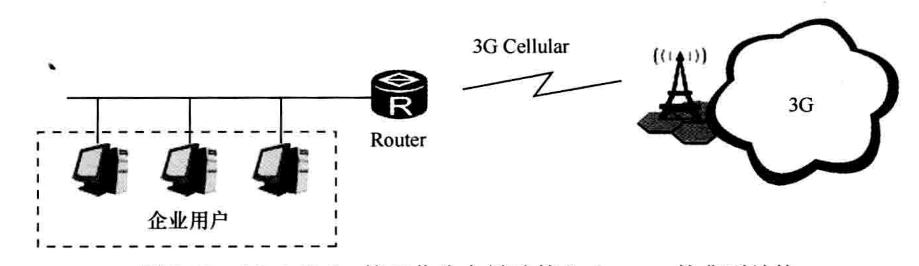


图 3-17　3G Cellular 接口作为主链路接入 Internet 的典型结构

（2）3G Cellular 接口作为备份链路接入 Internet

如图 3-18 所示，AR G3 系列路由器是企业的出口网关，企业通过 ADSL 接口作为主链路上行接入 Internet。为了增强企业接入 Internet 的可靠性，防止主链路发生故障导致企业用户无法正常接入 Internet，企业希望使用 3G Cellular 接口作为备份链路上行接入 Internet。

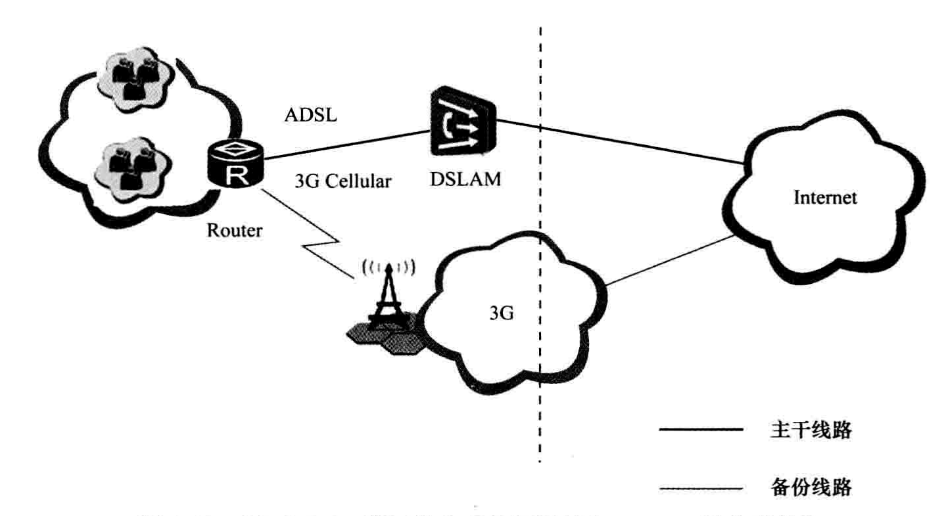


图 3-18 3G Cellular 接口作为备份链路接入 Internet 的典型结构

（3）3G Cellular 接口作为主备链路接入 Internet

如图 3-19 所示，AR G3 系列路由器是企业的出口网关，企业采取 3G Cellular 接口作为主备双条链路上行接入 Internet。

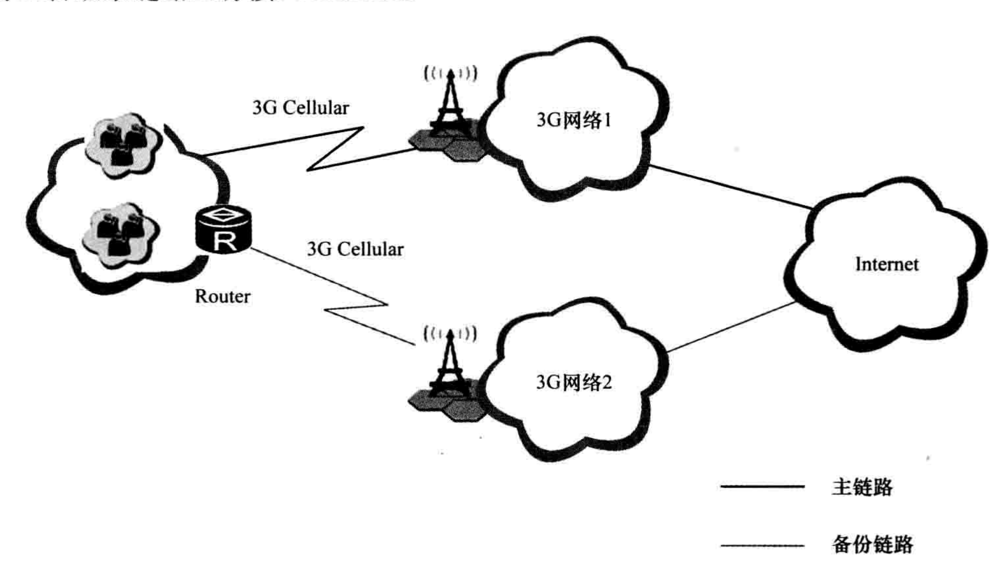


图 3-19 3G Cellular 接口作为主备链路接入 Internet 的典型结构

3.8.2 配置 WCDMA 网络中的 3G Cellular 接口

配置 3G Cellular 接口，用户可以通过 WCDMA 网络接入 Internet。当然在配置 3G Cellular 接口之前，需确保 3G Modem 和 SIM 卡在位。

1. 主要配置任务

WCDMA 网络的 3G Cellular 接口所需进行的主要配置任务如下。

（1）（可选）配置 MTU

设置 3G Cellular 接口的 MTU 值。这样当数据到达 3G Cellular 接口网络层时，会把

MTU 值与要发送的 IP 数据包的长度进行比较，如果 IP 数据包的长度比 MTU 值大，那么 IP 数据包就需要进行分片，分片后的数据包长度小于等于 MTU。

（2）配置 APN

APN（Access Point Name，访问点名称）用来标识 WCDMA 网络的业务种类，WCDMA 系统根据用户连接 WCDMA 网络的 APN 提供相应的服务。

用户可以使用参数描述模板来配置 APN。但不同 WCDMA 网络运营商的 APN 不同，APN 的获取需要咨询当地运营商。配置 APN 后，APN 会记录在 3G Modem 中，以后会一直存在。如果 APN 值变化，需要重新配置。

（3）（可选）配置选择 PLMN

对于 WCDMA 网络，用户可以采用自动或手动的方式选择 PLMN（Public Land Mobile Network，公网陆地移动网络）。

缺省情况下，采用自动方式选择 PLMN。当你购买网络运营商的 WCDMA 服务，并且从网络运营商获取 MCC（Mobile Country Code，移动国家代码）和 MNC（Mobile Network Code，移动网络代码）时，可以采用手动方式选择 PLMN。

（4）配置网络连接方式

3G Modem 有多种类型，不同类型的 3G Modem 连接 WCDMA 网络有各自的缺省方式。另外，配置 3G Modem 连接 WCDMA 网络的方式后，该配置会记录在 3G Modem 中，并将长期有效。

请确认 3G Modem 连接 WCDMA 网络的方式与运营商提供的 WCDMA 网络是否一致。如果不一致，你需要执行本配置任务更改 3G Modem 连接 WCDMA 网络的方式。

（5）配置轮询 DCC 拨号连接

WCDMA 网络拨号方式可以分为以下两种。

① 自动拨号（永久在线方式）。

在设备启动后，DCC 自动尝试拨号连接对端，无需通过数据报文进行触发。若无法与对端正常建立拨号连接，则每隔一段时间 DCC 将再次自动尝试建立拨号连接。

自动拨号方式适用于不计流量、不计时间的场合。比如包年业务，在规定时间内，该链路无流量和使用时间限制。

② 按需拨号（非永久在线，流量触发链路建立）。

只有存在数据需要传送时，设备才会触发建立链路。当链路没有流量的时间到达超时时间后，设备会拆除链路，以节约流量。

按需拨号方式适用于对流量和链路使用时间敏感的场合。比如包流量业务，在某一个时间段内，允许使用一定流量。

（6）配置 PIN 管理功能

在移动网络中使用 PIN（Personal Identification Number，个人识别码）识别 SIM/UIM 卡使用者的身份，防止 SIM/UIM 卡被非法使用。

为了确保用户信息安全，如果连续三次输入错误的 PIN 码，则 SIM/UIM 卡会被锁住，需要使用 PUK（Personal Identification Number UnBlock Key）码才能解锁 SIM/UIM 卡。

说明 PIN码由4至8位十进制整数组成。通常由运营商设置初始PIN码，初始PIN码请咨询运营商。PUK码由运营商提供。当连续输入10次错误PUK码，该SIM/UIM卡会被永久锁住，只能去运营商更换SIM/UIM卡。

（7）（可选）屏蔽3G Cellular接口

当设备管理员出于信息安全考虑，希望普通用户不能使用设备的3G功能进行通信时，可以屏蔽设备上的3G Cellular接口，从而使普通用户不能使用3G功能。

2. 具体配置步骤

以上各项配置任务的具体配置步骤如表3-21所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表3-21　　WCDMA网络中的3G Cellular接口配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：<Huawei>**system- view**	进入系统视图
	2	**interface cellular** *interface-number* 例如：[Huawei] **interface cellular** 0/0/0	进入3G Cellular接口视图
（可选）配置MTU	3	**mtu** *mtu* 例如：[Huawei-Cellular0/0/ 0] **mtu** 1200	配置3G Cellular接口的MTU，取值范围是128～1 500整数个字节。执行完本命令后，请执行**shutdown**和**undo shutdown**或**restart**命令，重新启动相应的物理接口，使配置生效。且如果在同一个3G Cellula接口视图下重复执行**mtu**命令时，新配置将覆盖老配置 缺省情况下，3G Cellular接口的MTU是1 500字节，可用**undo mtu**命令恢复为缺省情况
配置APN	4	**profile create** *profile-number* { **dynamic** | **static** *apn* } 例如：[Huawei-Cellular0/0/0] **profile create 1 static** 3GNET	创建3G Modem的参数描述模板并配置APN。命令中的参数和选项说明如下 ● *profile-number*：指定所创建的参数描述模板的索引值，取值只能为1 ● **dynamic**：二选一选项，指定创建设备动态配置APN ● **static** *apn*：二选一参数，指定创建用户手工配置APN，参数用来指定创建的用户APN序号，1～99个字符，不支持空格，区分大小写。不同WCDMA网络运营商的APN不同，APN的获取需要咨询当地运营商
（可选）配置选择PLMN	5	**plmn search** 例如：[Huawei-Cellular0/0/0] **plmn search**	配置搜索PLMN。本命令不属于配置命令，属于一种网络探测命令，用来搜索公共陆地移动网络。搜索到PLMN后，设备将显示搜索结果，用户可以根据搜索结果执行下面的**plmn select**命令配置手动方式选择PLMN（对于WCDMA网络，用户可以采用自动或手动的方式选择PLMN）

（续表）

<table>
<tr><th>配置任务</th><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td rowspan="2">（可选）
配置选择
PLMN</td><td rowspan="2">6</td><td>plmn auto</td><td colspan="2">（二选一）配置采用自动方式选择 PLMN</td></tr>
<tr><td>plmn select manual mcc mnc</td><td colspan="2">（二选一）配置采用手动方式选择 PLMN，命令中的 mcc 用来指定移动国家编码，取值范围为 0～65 535 的整数，mnc 用来指定移动网络编码，取值范围为 0～65 535 的整数</td></tr>
<tr><td rowspan="2">配置网络
连接方式</td><td>7</td><td>mode wcdma { gsm-only | gsm-precedence | wcdma-only | wcdma-precedence }
例如：[Huawei-Cellular0/0/0] mode wcdma wcdma-only</td><td colspan="2">配置为 WCDMA 网络连接方式。命令中的选项说明如下
● gsm-only：多选一选项，指定 3G Modem 只选择 GSM 网络
● gsm-precedence：多选一选项，指定 3G Modem 优先选择 GSM 网络
● wcdma-only：多选一选项，指定 3G Modem 只选择 WCDMA 网络
● wcdma-precedence：多选一选项，指定 3G Modem 优先选择 WCDMA 网络
如果在同一个 3G Cellular 接口视图下重复执行 mode wcdma 命令且参数不同时，则新配置将覆盖老配置</td></tr>
<tr><td>8</td><td>quit
例如：[Huawei-Cellular0/0/0] quit</td><td colspan="2">退出 3G Cellular 接口视图，返回系统视图</td></tr>
<tr><td rowspan="2">配置轮询
DCC 拨号
连接</td><td>9</td><td>dialer-rule
例如：[Huawei] dialer-rule</td><td rowspan="2">配置拨号
控制列表</td><td>进入 Dialer-rule 视图。在需要配置拨号访问控制列表时，需要使用本命令先进入 Dialer- rule 视图</td></tr>
<tr><td>10</td><td>dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny | permit } | ipv6 { deny | permit } }
例如：[Huawei-dialer-rule] dialer-rule 1 ip permit</td><td>配置某个拨号访问组对应的拨号访问控制列表，指定引发 DCC 呼叫的条件。命令中的参数和选项说明如下
● dialer-rule-number：指定拨号访问组的编号，取值范围为 1～255 的整数。取值要与下面 dialer-group 命令中的 group-number 参数值一致
● acl { acl-number |name acl-name }：多选一选项，指定配置的拨号访问控制列表过滤报文时需要满足的 ACL 编号或 ACL 名称
● ip { deny |permit }：多选一选项，指定配置的拨号访问控制列表禁止或允许 IPv4 协议的数据报文
● ipv6 { deny |permit }：多选一选项，指定配置的拨号访问控制列表禁止或允许 IPv6 协议的数据报文
缺省情况下，未配置任何拨号访问控制列表，可用 undo dialer-rule dialer-rule-number [acl | ip | ipv6] 命令取消对应拨号访问组的拨号访问控制设置</td></tr>
</table>

（续表）

配置任务	步骤	命令	说明	
配置轮询DCC拨号连接	11	**quit** 例如：[Huawei-dialer-rule] **quit**	配置拨号控制列表	退出Dialer-rule视图，返回系统视图
	12	**interface cellular** *interface-number* 例如：[Huawei] **interface cellular** 0/0/0	使能轮询DCC	进入3G Cellular接口视图
	13	**ip tcp vjcompress** 例如：[Huawei-Cellular0/0/0] **ip tcp vjcompress**		配置接口的VJHC压缩功能。VJHC是一种应用在PPP链路上的TCP/IP报头压缩算法，符合RFC1144协议。PPP通过IPCP（IP Compression Protocol）来协商使用VJHC压缩，以提高PPP链路传输效率。如果需要两个方向都进行压缩则需要PPP链路双方独立申请 缺省情况下，接口未配置VJHC压缩功能，可用**undo ip tcp vjcompress**命令删除PPP链路接口的VJHC压缩功能
	14	**dialer enable-circular** 例如：[Huawei-Cellular0/0/0] **dialer enable-circular**		使能轮询DCC功能。轮询DCC适用于物理链路较多，连接情况复杂的大中型站点 缺省情况下，接口上未使能轮询DCC功能，可用**undo dialer enable-circular**命令去使能轮询DCC功能
	15	**dialer-group** *group-number* 例如：[Huawei-Cellular0/0/0] **dialer-group** 1		指定接口所属的拨号访问组的编号，这个拨号访问组由**dialer-rule**命令设定，取值范围是1～255的整数 缺省情况下，未配置DCC拨号控制列表及拨号接口所属的拨号访问组，可用**undo dialer-group**命令将接口从此拨号访问组中删除
	16	**ip address ppp-negotiate** 例如：[Huawei-Cellular0/0/0] **ip address ppp-negotiate**	配置接入验证（建议同时配置PAP和CHAP认证）	配置本端接口接受PPP协商产生的由对端分配的IP地址。若本端接口封装的链路层协议为PPP但还未配置IP地址，而对端已有IP地址时，可为本端接口配置IP地址可协商属性，使本端接口接受PPP协商产生的由对端分配的IP地址。这种方式主要用在通过ISP（Internet Service Provider）访问Internet时，获得由ISP分配的IP地址 缺省情况下，接口不通过PPP协商获取IP地址，可用**undo ip address ppp-negotiate**命令取消接口通过PPP协商获取IP地址

（续表）

配置任务	步骤	命令		说明
配置轮询DCC拨号连接	17	**ppp ipcp dns request** 例如：[Huawei-Cellular0/0/0] **ppp ipcp dns request**	配置接入验证（建议同时配置PAP和CHAP认证）	（二选一）配置接口可以接收对端分配的 DNS 服务器地址。配置设备主动请求对端指定 DNS 服务器地址。 当设备通过 PPP 与其他设备相连时，若设备需要通过域名直接访问 Internet，则需要对端设备为其分配 DNS 服务器地址。要使对端设备能够为本设备分配 DNS 服务器地址，可以使用本命令配置本设备主动向对端请求 DNS 服务器地址或使用下面将要介绍的 **ppp ipcp dns admit-any** 命令配置本设备被动地接收对端设备指定的 DNS 服务器的 IP 地址 缺省情况下，禁止设备主动向对端请求 DNS 服务器地址，可用 **undo ppp ipcp dns request** 命令恢复为缺省值
		ppp ipcp dns admit-any 例如：[Huawei-Cellular0/0/0] **ppp ipcp dns admit-any**		（二选一）配置接口可以接收对端分配的 DNS 服务器地址。配置设备被动地接收对端指定的 DNS 服务器地址。 缺省情况下，设备不会被动地接收对端设备指定的 DNS 服务器的 IP 地址，可用 **undo ppp ipcp dns admit-any** 命令禁止设备被动地接收对端设备指定的 DNS 服务器的 IP 地址
	18	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password* 例如：[Huawei-Cellular0/0/0] **ppp pap local-user** papuser1 **password simple** huawei		配置本地被对端以 PAP 方式验证时本地发送的 PAP 用户名和密码。 命令中的参数和选项说明如下。 ● *username*：指定用于被对端设备进行 PAP 方式认证时的用户名，1～64 个字符，支持空格，区分大小写 ● **cipher**：二选一选项，指定密码为密文显示 ● **simple**：二选一选项，指定密码为明文显示 ● *password*：指定本地设备被对端设备采用 PAP 方式认证时发送的口令，支持空格，区分大小写，如果选择 **simple**，则 *password* 必须是明文密码，长度范围是 1～32 个字符；如果选择 **cipher**，则 *password* 可以是长度范围是 24～56 位的密文密码，也可以是长度范围为 1～32 位的明文密码 缺省情况下，被对端以 PAP 方式验证时，本地设备发送的用户名和口令均为空，可用 **undo ppp pap local-user** 命令取消配置的用户名和口令

（续表）

配置任务	步骤	命令	说明	
配置轮询 DCC 拨号连接	19	**ppp chap user** *username* 例如：[Huawei-Cellular0/0/0] **ppp chap user** huawei **ppp chap password** { **cipher** | **simple** } *password* 例如：[Huawei-Cellular0/0/0] **ppp chap password simple** huawei	配置接入验证（建议同时配置 PAP 和 CHAP 认证）	配置 CHAP 方式验证。配置 CHAP 认证的用户名和密码。两命令中的参数和选项说明如下 • *username*：设置 CHAP 验证的用户名，该用户名是发送到对端设备进行 CHAP 验证时使用的用户名，1～64 个字符，不支持空格，区分大小写 • **cipher**：二选一选项，指定密码为密文显示 • **simple**：二选一选项，指定密码为明文显示 • *password*：指定 CHAP 认证的口令，支持空格，区分大小写，如果选择 **simple**，则 *password* 必须是明文密码，长度范围是 1～32 个字符；如果选择 **cipher**，则 *password* 可以是长度范围是 24～56 位的密文密码，也可以是长度范围是 1～32 位的明文密码 缺省情况下，CHAP 认证的用户名为空，可用 **undo ppp chap user** 命令删除 CHAP 验证的用户名 缺省情况下，未配置 CHAP 验证的口令，可用 **undo ppp chap password** 命令删除配置的口令
	20	**dialer number** *dial-number* [**autodial**] 例如：[Huawei-Cellular0/0/0] **dialer number** 1111	配置轮询 DCC 呼叫	配置呼叫一个对端的拨号串，**通常也就是要拨的电话号码**。命令中的参数和选项说明如下 • *dial-number*：1～30 个字符，不支持空格，区分大小写，指定该接口下呼叫一个对端的拨号串 • **autodial**：可选项，配置接口根据拨号串自动拨号，如果不选此可选项，则表示为按需拨号 拨号串由运营商提供，请向运营商获取
配置 PIN 管理功能	21	**pin verification enable** *pin* 例如：[Huawei-Cellular0/0/0] **pin verification enable** 1234	使能 3G Modem 的 PIN 码认证功能。为了防止非法用户擅自使用 SIM/UIM 卡，用户可以使能 3G Modem 的 PIN 码认证功能，这样没有通过 PIN 码认证的用户无法使用 3G Modem 进行数据通信。参数 *pin* 用来指定插在 3G Modem 上的 SIM/UIM 卡的 PIN 码，由 4～8 位十进制整数组成。通常由运营商设置初始 PIN 码，用户自己可以修改 PIN 码 缺省情况下，PIN 码认证功能处于未使能状态	

（续表）

配置任务	步骤	命令	说明
配置 PIN 管理功能	22	**pin verify** *pin* 例如：[Huawei-Cellular0/0/0] **pin verify** 1234	对 PIN 码进行认证。使能 PIN 码认证功能后，后续每次启动 SIM/UIM 卡时，设备都会要求用户对 PIN 码进行认证，否则 3G Modem 数据通信功能不可用
	23	**pin modify** *current-pin new-pin* 例如：[Huawei-Cellular0/0/0] **pin modify** 24567	修改 SIM/UIM 卡的 PIN 码。命令中的 *current-pin* 参数是指当前的 PIN 码，参数 *new-pin* 是指新修改后的 PIN 码，均由 4～8 位十进制整数组成 定期修改 PIN 码可以提高 SIM/UIM 卡的安全性
	24	**pin unlock** *puk new-pin* 例如：[Huawei-Cellular0/0/0] Huawei-Cellular0/0/0]**pin unlock** 87654321 12345	使用 PUK 码解锁 SIM/UIM 卡并重新设置 PIN 码。命令中的 *puk* 参数是指定插在 3G Modem 上的 SIM/UIM 卡的 PUK 码，*new-pin* 参数是要设置的新 PIN 码，均由 4～8 位十进制整数组成 PIN 解锁码 PUK（Personal Identification Number UnBlock Key，个人标识数字解锁码）通常由网络运营商提供。为了确保用户信息安全，如果用户连续三次输入错误的 PIN 码，则 SIM/UIM 卡会被锁住，需要使用 PUK 码才能解锁 SIM/UIM 卡。当连续输入 10 次错误的 PUK 码，该 SIM/UIM 卡会被永久锁住，只能去运营商处更换 SIM/UIM 卡
（可选）屏蔽 3G Cellular 接口	25	**quit**	退出 3G Cellular 接口视图，返回系统视图
	26	**remove interface-cellular**	屏蔽设备上的 3G Cellular 接口
	27	**quit**	返回用户视图
	28	**reboot**	重启路由器。重启后，屏蔽设备上的 3G Cellular 接口的配置才能生效

3.8.3 配置 CDMA2000 网络的 3G Cellular 接口

配置 3G Cellular 接口，用户可以通过 CDMA2000 网络连接到 Internet。当然在配置 3G Cellular 接口之前，需确保 3G Modem 和 UIM 卡在位。

1. 主要配置任务

针对 CDMA2000 网络的 3G Cellular 接口主要配置任务如下。

①（可选）配置 MTU：参见 3.8.2 小节介绍。

② 配置网络连接方式：参见 3.8.2 小节介绍，不同的是这里要选择的 3G 网络连接方式为 CDMA2000。另外，配置 3G Modem 连接 CDMA2000 网络的方式后，该配置会记录在 3G Modem 中，并将长期有效。

③ 配置轮询 DCC 拨号连接：参见 3.8.2 小节介绍。

④ 配置 PIN 管理功能：参见 3.8.2 小节介绍。

⑤（可选）屏蔽 3G Cellular 接口：参见 3.8.2 小节介绍。

对比上节介绍的 WCDMA 网络的 3G Cellular 接口主要配置任务，可以发现稍微简单些（不需要配置 APN 和 PLMN），而且相同配置任务中的绝大多数是与 WCDMA 网络的 3G Cellular 接口中的配置是完全一样的。

2. 具体配置步骤

以上各项配置任务的具体配置步骤如表 3-22 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序）。**

表 3-22 **CDMA2000 网络中的 3G Cellular 接口配置步骤**

<table>
<tr><th>配置任务</th><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td rowspan="2">公共配置</td><td>1</td><td>system-view
例如：< Huawei > system-view</td><td colspan="2">进入系统视图</td></tr>
<tr><td>2</td><td>interface cellular interface-number
例如：[Huawei] interface cellular 0/0/0</td><td colspan="2">进入 3G Cellular 接口视图</td></tr>
<tr><td>（可选）配置 MTU</td><td>3</td><td>mtu mtu
例如：[Huawei-Cellular0/0/0] mtu 1200</td><td colspan="2">配置 3G Cellular 接口的 MTU，取值范围是 128～1 500 整数个字节。其他说明参见 3.8.2 小节表 3-21 中第 3 步说明</td></tr>
<tr><td rowspan="2">配置网络连接方式</td><td>4</td><td>mode cdma { 1xrtt-only | evdo-only | hybrid }
例如：[Huawei-Cellular0/0/0] mode cdma hybrid</td><td colspan="2">配置为 CDMA2000 网络连接方式。命令中的选项说明如下。
● 1xrtt-only：多选一选项，指定 3G Modem 只选择 1xRTT 网络
● evdo-only：多选一选项，指定 3G Modem 只选择 EV-DO 网络
● hybrid：多选一选项，指定 3G Modem 选择 1xRTT 和 EV-DO 混合网络
请确认 3G Modem 连接 CDMA2000 网络的方式与运营商提供的 CDMA 网络一致。如果不一致，请使用本命令进行修改
如果在同一个 3G Cellular 接口视图下重复执行 mode cdma 命令且参数不同时，则新配置将覆盖老配置</td></tr>
<tr><td>5</td><td>quit
例如：[Huawei-Cellular0/0/0] quit</td><td colspan="2">退出 3G Cellular 接口视图，返回系统视图</td></tr>
<tr><td rowspan="5">配置轮询 DCC 拨号连接</td><td>6</td><td>dialer-rule
例如：[Huawei] dialer-rule</td><td rowspan="3">配置拨号控制列表</td><td>进入 Dialer-rule 视图。在需要配置拨号访问控制列表时，需要使用本命令先进入 Dialer-rule 视图</td></tr>
<tr><td>7</td><td>dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny | permit } | ipv6 { deny | permit } }
例如：[Huawei-dialer-rule] dialer-rule 1 ip permit</td><td>配置某个拨号访问组对应的拨号访问控制列表，指定引发 DCC 呼叫的条件。其他说明参见 3.8.2 小节表 3-21 中第 10 步说明</td></tr>
<tr><td>8</td><td>quit
例如：[Huawei-dialer-rule]</td><td>退出 Dialer-rule 视图，返回系统视图</td></tr>
<tr><td>9</td><td>interface cellular interface-number
例如：[Huawei] interface cellular 0/0/0</td><td rowspan="2">使能轮询 DCC</td><td>进入 3G Cellular 接口视图</td></tr>
<tr><td>10</td><td>ip tcp vjcompress
例如：[Huawei-Cellular0/0/0] ip tcp vjcompress</td><td>配置接口的 VJHC 压缩功能。其他说明参见 3.8.2 小节表 3-21 中第 13 步说明</td></tr>
</table>

（续表）

配置任务	步骤	命令	说明	
配置轮询 DCC 拨号连接	11	**dialer enable-circular** 例如：[Huawei-Cellular0/0/0] **dialer enable-circular**	使能轮询 DCC	使能轮询 DCC 功能。其他说明参见 3.8.2 小节表 3-21 中第 14 步说明
	12	**dialer-group** *group-number* 例如：[Huawei-Cellular0/0/0] **dialer-group** 1		指定接口所属的拨号访问组的编号，其他说明参见 3.8.2 小节表 3-21 中第 15 步说明
	13	**ip address ppp-negotiate** 例如：[Huawei-Cellular0/0/0] **ip address ppp-negotiate**	配置接入验证（建议同时配置 PAP 和 CHAP 认证）	配置本端接口接受 PPP 协商产生的由对端分配的 IP 地址。其他说明参见 3.8.2 小节表 3-21 中第 16 步说明
	14	**ppp ipcp dns request** 例如：[Huawei-Cellular0/0/0] **ppp ipcp dns request**		（二选一）配置接口可以接收对端分配的 DNS 服务器地址。其他说明参见 3.8.2 小节表 3-21 中第 17 步说明
		ppp ipcp dns admit-any 例如：[Huawei-Cellular0/0/0] **ppp ipcp dns admit-any**		（二选一）配置接口可以接收对端分配的 DNS 服务器地址。其他说明参见 3.8.2 小节表 3-21 中第 17 步说明
	15	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password* 例如：[Huawei-Cellular0/0/0] **ppp pap local-user** papuser1 **password simple** huawei		配置本地被对端以 PAP 方式验证时本地发送的 PAP 用户名和密码。其他说明参见 3.8.2 小节表 3-21 中第 18 步说明
	16	**ppp chap user** *username* 例如：[Huawei-Cellular0/0/0] **ppp chap user** huawei **ppp chap password** { **cipher** | **simple** } *password* 例如：[Huawei-Cellular0/0/0] **ppp chap password simple** huawei		配置 CHAP 方式验证。配置 CHAP 认证的用户名和密码。其他说明参见 3.8.2 小节表 3-21 中第 19 步说明
	17	**dialer number** *dial-number* [**autodial**] 例如：[Huawei-Cellular0/0/0] **dialer number** 1111	配置轮询 DCC 呼叫	配置呼叫一个对端的拨号串。其他说明参见 3.8.2 小节表 3-21 中第 20 步说明
配置 PIN 管理功能	18	**pin verification enable** *pin* 例如：[Huawei-Cellular0/0/0] **pin verification enable** 1234	使能 3G Modem 的 PIN 码认证功能。其他说明参见 3.8.2 小节表 3-21 中第 21 步说明	
	19	**pin verify** *pin* 例如：[Huawei-Cellular0/0/0] **pin verify** 1234	对 PIN 码进行认证。使能 PIN 码认证功能后，后续每次启动 SIM/UIM 卡时，设备都会要求用户对 PIN 码进行认证，否则 3G Modem 数据通信功能不可用	
	20	**pin modify** *current-pin new-pin* 例如：[Huawei-Cellular0/0/0] **pin modify** 24567	修改 SIM/UIM 卡的 PIN 码。其他说明参见 3.8.2 小节表 3-21 中第 23 步说明	
	21	**pin unlock** *puk new-pin* 例如：[Huawei-Cellular0/0/0] Huawei-Cellular0/0/0] **pin unlock** 87654321 12345	使用 PUK 码解锁 SIM/UIM 卡并重新设置 PIN 码。其他说明参见 3.8.2 小节表 3-21 中第 24 步说明	

（续表）

配置任务	步骤	命令	说明
（可选）屏蔽 3G Cellular 接口	22	**quit**	退出 3G Cellular 接口视图，返回系统视图
	23	**remove interface-cellular**	屏蔽设备上的 3G Cellular 接口
	24	**quit**	返回用户视图
	25	**reboot**	重启路由器。重启后，屏蔽设备上的 3G Cellular 接口的配置才能生效

3.8.4 3G Cellular 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 3G Cellular 接口，也可用以下 **reset** 用户视图命令清除 3G Cellular 接口上的统计信息（当你需要统计一定时间内 3G Cellular 接口生成的串口的流量信息时，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display cellular** *interface-number* **all**：查看 3G Modem 的呼叫连接信息，包括硬件信息、参数描述模板信息、网络信息、无线信息和安全信息。

② **display interface cellular** [*interface-number*]：查看 3G Cellular 接口当前运行状态和接口统计信息。

③ **reset counters interface cellular** [*interface-number*]：清除当前 3G Cellular 接口的统计信息。

3G Modem 在运行过程中能够自动检测异常，并实施自动重启。如果 3G Modem 无法自动重启，用户可以在 3G Cellular 接口视图下使用 **modem reboot** 命令手动重启 3G Modem。



SIM/UIM 卡不支持热插拔。

① 对于由外置 3G Modem 的 USB 接口或内置 3G Modem 的 3G-HSPA+7 接口卡提供的 3G Cellular 接口，为了保证插入的 SIM/UIM 卡正常工作，热拔插 SIM/UIM 卡后，需要手动重启 3G Modem。

② 对于 AR151G-HSPA+7、AR157G-HSPA+7 和 AR207G-HSPA+7 机型，当其 3G Cellular 接口由外置 3G Modem 的 USB 接口提供时，热拔插 SIM/UIM 卡后，需要手动重启 3G Modem；当其 3G Cellular 接口既不由外置 3G Modem 的 USB 接口提供，而是使用设备本身就支持的 3G Cellular 接口时，热拔插 SIM/UIM 卡后，需要手动重启该设备。

3.8.5 WCDMA 网络中 3G Cellular 接口作为主链路接入 Internet 的配置示例

本示例的拓扑结构如图 3-20 所示，AR G3 路由器使用 Ethernet2/0/0 接口连接企业内网用户，使用 3G Cellular 接口通过 WCDMA 网络接入 Internet。已知企业办理了每月 10G 的流量业务，采用按需拨号方式接入 Internet。企业从运营商获取到的信息如下。

① 用户名和密码为 3guser 和 Password123。

② APN 为 3GNET。

③ 拨号串为*99#。

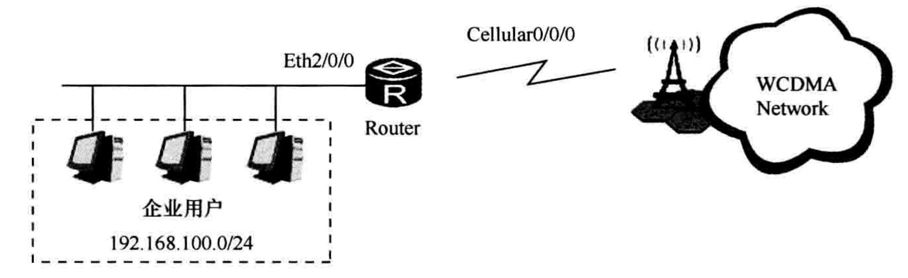


图 3-20　WCDMA 网络中 3G Cellular 接口作为主链路接入 Internet 的配置示例基本网络结构

1. 基本配置思路分析

本示例的最终要求就是企业网络用户能够通过 3G Cellular 接口连接的 WCDMA 网络接入 Internet。要实现这一目标，主要需要配置两个方面：一是配置按需拨号的 3G 功能，使企业可以利用 3G 业务接入 Internet；二是配置以 Cellular0/0/0 为出接口的缺省路由，使企业内网的流量通过 3G Cellular 接口上行传输到 Internet。当然，在企业内网用户主机上还要以路由器的 LAN 口 Ethernet2/0/0 作为网关。下面仅介绍前两项配置任务。

（1）配置按需拨号的 3G 功能

对照 3.8.2 小节介绍的配置任务可以知道，三个可选任务是不用配置的，仅需配置以下 4 项任务：APN、网络连接方式、轮询 DCC 拨号连接和 PIN 管理。

① 配置 APN，用来标识 WCDMA 网络的业务种类，WCDMA 系统根据用户连接 WCDMA 网络的 APN 提供相应的服务。

```
[Router] interface cellular 0/0/0
[Router-Cellular0/0/0] profile create 1 static 3GNET  !--- 创建 3G Modem 的参数描述模板 1，并手工创建一个名为 3GNET 的 APN
```

② 配置 3G Modem 连接 WCDMA 网络的方式，此处假设以 WCDMA 优先方式。

```
[Router-Cellular0/0/0] mode wcdma wcdma-precedence
[Router-Cellular0/0/0] quit
```

③ 配置按需拨号（这是本示例要求的）。其中包括配置拨号控制列表、使能轮询 DCC、配置接入验证和配置轮询 DCC 呼叫。

- 配置拨号控制列表。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dialer-rule                              !--- 进入 Dialer-rule 视图
[Router-dialer-rule] dialer-rule 1 ip permit      !---配置一条允许 IPv4 通信的访问控制列表规则
[Router-dialer-rule] quit
```

- 配置接入验证。

```
[Router] interface cellular 0/0/0
[Router-Cellular0/0/0] link-protocol ppp
[Router-Cellular0/0/0] ip address ppp-negotiate              !---配置 cellular 0/0/0 接口采用 PPP 协商 IP 地址
[Router-Cellular0/0/0] ppp ipcp dns request                  !---配置 cellular 0/0/0 接口采用 PPP 协商 DNS 服务器地址
[Router-Cellular0/0/0] ppp chap user 3guser                  !---配置 CHAP 认证用户名为 3guser
[Router-Cellular0/0/0] ppp chap password cipher Password123 !---配置 CHAP 认证用户密码为 Password123
```

- 使能轮询 DCC。

```
[Router-Cellular0/0/0] dialer enable-circular
[Router-Cellular0/0/0] dialer-group 1  !---配置 3G Cellular0/0/0 接口拨号访问组编号，要与控制列表规则中对应的拨号访问组编号一致
```

- 配置轮询 DCC 呼叫。

```
[Router-Cellular0/0/0] dialer number *99#   !--- 配置呼叫对端的拨号串为*99#
```

（2）配置缺省路由，指定出接口为 Cellular0/0/0

```
[Router] ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/0
```

配置好后，可以通过 **display interface** Cellular 0/0/0 命令查看接口的详细信息，验证配置结果。正常情况下，当接口上有流量传送时，可以看到接口的物理层和链路层的状态都是 Up、PPP 的 LCP 和 IPCP 都处于 opened 状态，PPP 协商获得的 IP 地址为 20.1.1.2/24（**如输出信息中的粗体字部分所示**），这说明链路的 PPP 协商已经成功。具体如下。

```
[Router] display interface Cellular 0/0/0
Cellular0/0/0 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Cellular0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is negotiated, 20.1.1.2/24
Link layer protocol is PPP
LCP opened, IPCP opened
Current system time: 2011-06-08 11:35:23
Modem State: Present
Last 300 seconds input rate 555 bytes/sec 4 440 bits/sec 12 packets/sec
Last 300 seconds output rate 11 230 bytes/sec 89 840 bits/sec 311 packets/sec
    Input: 210 packets, 87 205 bytes
    Output:225340 packets, 6 760 917 bytes
    Input bandwidth utilization    : 0.01%
    Output bandwidth utilization : 0.01%
```

还可以通过 **display Cellular** 0/0/0 **all** 命令查看 3G Modem 的呼叫连接信息，可以看到 APN 为 3GNET、无线网络类型为 WCDMA 以及网络连接方式为 WCDMA precedence（**如输出信息中的粗体字部分所示**）。

```
[Router] display Cellular 0/0/0 all
Modem State:
Hardware Information.
=====================
Model = K4505
Modem Firmware Version = 11.870.02.10.11
Hardware Version = "CP12TCPU"
International Mobile Subscriber Identity (IMSI) = 460016002707237
International Mobile Equipment Identity (IMEI) = 354661034412719
Factory Serial Number (FSN) = MLA7NA1093003693
Modem Status = Online
Profile Information.
=====================
Profile 1 = ACTIVE
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 3GNET
Packet Session Status = Active
* - Default profile
Network Information.
=====================
Current Service Status = Service available
Current Service = Combined
```

```
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Home
Network Selection Mode = Automatic
Network Connection Mode = WCDMA precedence
Current Network Connection = WCDMA(WCDMA)
Mobile Country Code (MCC) = 460
<省略>
```

3.8.6 WCDMA 网络中 3G Cellular 接口作为主备链路接入 Internet 的配置示例

本示例拓扑结构如图 3-21 所示，RouterA 是某企业的出口网关。正常情况下，RouterA 通过 3G 网络 1 接入 Internet。为了防止因 3G 接口 Cellular0/0/0 或 3G 网络 1 故障而导致企业用户无法连接到 Internet，企业租用了一条通过 3G 网络 2 接入 Internet 的备份链路，希望实现当 Cellular0/0/0 或 3G 网络 1 故障时，使用备份链路临时承担业务传输。

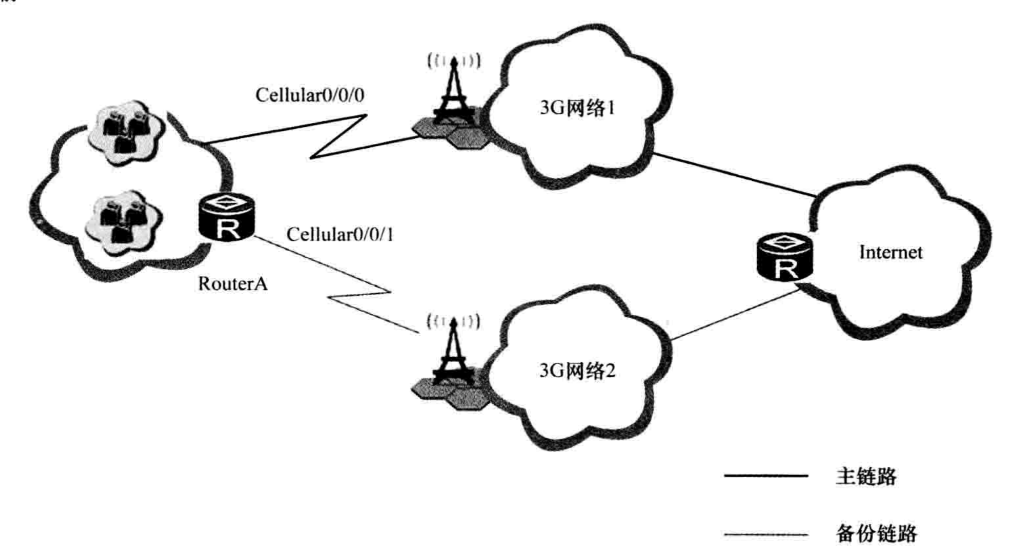


图 3-21 WCDMA 网络中 3G Cellular 接口作为主备链路接入 Internet 的配置示例基本网络结构

本示例假设 3G 网路 1 的网络连接方式为 WCDMA，APN 为 3GNET，拨号串为*99#；3G 网络 2 的网络连接方式为 CDMA2000，拨号串为#777。

1. 基本配置思路分析

本示例其实就是两种 3G 网络接入的配置，其中一个作为主接入线路，另一个作为备用接入线路。基本的配置思路如下。

① 在 RouterA 上配置 3G 接口 Cellular0/0/0，实现 RouterA 通过 3G 网络 1 接入 Internet。

② 在 RouterA 上配置 3G 接口 Cellular0/0/1，实现 RouterA 通过 3G 网络 2 接入 Internet。

③ 配置 Cellular0/0/1 为 Cellular0/0/0 的备份接口，实现当主接口故障时，流量可以切换到备份接口 Cellular0/0/1 上。

④ 配置轮询 DCC，实现通过拨号使用主链路或备份链路接入 Internet。

⑤ 配置两条不同优先级的缺省路由，在实现网络层互通的同时实现线路主、备线路区分。

2．具体配置步骤。

① 配置 3G 接口 Cellular0/0/0。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface cellular 0/0/0
[RouterA-Cellular0/0/0] link-protocol ppp
[RouterA-Cellular0/0/0] ip address ppp-negotiate
[RouterA-Cellular0/0/0] profile create 1 static 3GNET   !---配置 APN
[RouterA-Cellular0/0/0] mode wcdma wcdma-precedence   !---配置 WCDMA 的网络连接方式
[RouterA-Cellular0/0/0] quit
```

② 配置 3G 接口 Cellular0/0/1。

```
[RouterA] interface cellular 0/0/1
[RouterA-Cellular0/0/1] link-protocol ppp
[RouterA-Cellular0/0/1] ip address ppp-negotiate
[RouterA-Cellular0/0/1] mode cdma hybrid   !---配置 CDMA 的网络连接方式
[RouterA-Cellular0/0/1] quit
```

③ 配置 3G **cellular 0/0/1** 接口为 3G Cellular0/0/0 的备份接口。

```
[RouterA] interface cellular 0/0/0
[RouterA-Cellular0/0/0] standby interface cellular 0/0/1
[RouterA-Cellular0/0/0] quit
```

④ 配置轮询 DCC。

```
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit !---配置拨号访问组 1 及其对应的许可 IPv4 通信的拨号访问控制条件，两个 3G Cellular 接口可以共享一个拨号访问组
[RouterA-dialer-rule] quit
!---以下是配置 3G Cellular0/0/0 接口使能轮询 DCC
[RouterA] interface cellular 0/0/0
[RouterA-Cellular0/0/0] dialer enable-circular
[RouterA-Cellular0/0/0] dialer-group 1
[RouterA-Cellular0/0/0] dialer timer autodial 60
[RouterA-Cellular0/0/0] dialer number *99# autodial
[RouterA-Cellular0/0/0] quit
!---以下是配置 3G Cellular0/0/1 接口使能轮询 DCC
[RouterA] interface cellular 0/0/1
[RouterA-Cellular0/0/1] dialer enable-circular
[RouterA-Cellular0/0/1] dialer-group 1
[RouterA-Cellular0/0/1] dialer timer autodial 60
[RouterA-Cellular0/0/1] dialer number #777 autodial
[RouterA-Cellular0/0/1] quit
```

⑤ 配置两条优先级不同的静态路由，实现 3G Cellular0/0/1 作 3G Cellular0/0/0 的备份线路。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/0 preference 40
[RouterA] ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/1 preference 80
```

配置完成后，在 RouterA 上执行 **display standby state** 检查主备接口状态，可以看到 Cellular0/0/0 接口的状态为 UP，备份接口 Cellular0/0/1 接口的状态为 STANDBY，如下面输出信息中的粗体字部分所示。

```
[RouterA] display standby state
Interface                    Interfacestate Backupstate Backupflag Pri    Loadstate
```

```
Cellular0/0/0                      UP          MUP        MU
Cellular0/0/1                      STANDBY     STANDBY      BU     0

 Backup-flag meaning:
 M---MAIN  B---BACKUP     V---MOVED     U---USED
 D---LOAD  P---PULLED
<省略>
```

现在配置 Cellular0/0/0 接口执行 **shutdown** 命令，模拟链路故障。在 RouterA 上执行 **display standby state** 检查主备接口状态，可以看到 Celllular0/0/0 的状态为 DOWN，备份接口 Cellular0/0/1 接口的状态为 UP，说明备份接口已被启用，如下面输出信息中的粗体字部分所示。

```
[RouterA-Cellular0/0/0] shutdown
[RouterA-Cellular0/0/0] quit
[RouterA] display standby state
Interface                    Interfacestate Backupstate Backupflag Pri   Loadstate
Cellular0/0/0                      DOWN        MDOWN             MU
Cellular0/0/1                      UP          UP            BU   0
<省略>
```

3.9　POS 接口配置与管理

POS（Packet Over SONET/SDH）接口可利用 SONET（Synchronous Optical Network，同步光纤网）或 SDH（Synchronous Digital Hierarchy，同步数字体系）提供的高速传输通道直接传送 IP 数据业务，广泛应用于城域网及广域网中。

在 AR G3 系列路由器中，POS 接口是由 1STM1 或 1STM4 接口卡提供，**仅有 AR2204/2204-S、AR2220L、AR2220/2220-S、AR2240 和 AR3260 支持 POS 接口。**

3.9.1　POS 接口简介

POS 是一种应用在城域网及广域网中的技术，利用 SONET/SDH 提供的高速传输通道直接传送 IP 数据业务。POS 使用链路层协议（FR、PPP 和 HDLC 等）对 IP 数据包进行封装，然后由 SONET/SDH 通道层的业务适配器把封装后的 IP 数据包映射到 SONET/SDH 同步净荷中，再把净荷装入一个 SONET/SDH 帧中，最后送达光网络中传输。

POS 接口使用 SONET/SDH 物理层传输标准，提供一种高速、可靠、点到点的 IP 数据连接。目前，在 AR G3 系列路由器中提供两种速率的 POS 接口，两种速率分别使用的信号等级是 OC-3/STM-1（155 Mbit/s）和 OC-12/STM-4（622 Mbit/s）。POS 在 SONET/SDH 网络中的典型应用基本网络结构如图 3-22 所示。



图 3-22　POS 接口典型应用基本网络结构

SDH 与 SONET 是两种同步传输体制，分别由不同的组织制定，两者除了在技术细节参数上有一些差别外，在实质内容和主要规范上并没有很大区别，但是两者应用的地域范围有所不同（SDH 主要应用于欧洲和中国，SONET 主要应用于北美和日本），不同设备厂商也有不同的缺省配置。

SONET 技术最早是由美国贝尔通信研究所提出的，后来成为 ANSI 定义的同步数字传输标准，主要应用于北美和日本。SONET 为光纤传输系统定义了同步传输的线路速率等级结构，其传输速率以 51.84 Mbit/s 为基础。在电信号中，此速率称为第 1 级同步传送信号（Synchronous Transport Signal），即 STS-1。STS-1 数据帧是 SONET 中传送的基本单元。在光信号中，此速率称为第 1 级光载波（Optical Carrier），即 OC-1。3 个 OC-1（STS-1）信号通过时分复用的方式复用成 SONET 层次的下一个级别 OC-3，速率为 155.520 Mbit/s。更高速率的电路由多个低级速率的电路连续汇聚构成，它们的速率总是可以从它们的名称上立即知道。例如，4 个 OC-3 或者 STS-1 电路可以复用构成一个 622.08 Mbit/s 的电路，其名称分别为 OC-12 或者 STS-4。

SDH 是以 SONET 为基础发展的新型光纤技术，并最终由 ITU-T 制订出对应的国际标准，主要应用于欧洲。SDH 和 SONET 绝大部分都是相同的，只是 SDH 的基本速率为 155.52 Mbit/s，称为第 1 级同步传递模块（Synchronous Transfer Module），即 STM-1。它相当于 SONET 体系中的 OC-3 速率。通过时分复用技术也可形成更高速率的 SDH 接入速率，即 STM-N，其速率是 STM-1 的 N 倍（N=4n=1，4，16，64，256）。

SONET 和 SDH 体制都能够用来封装较早的数字传输标准，比如 PDH（Plesiochronous Digital Hierarchy，准同步数字系列）标准，或者直接用来支持 ATM 以及所谓的 SONET 上的分组业务（Packet Over SONET）网络。

3.9.2 配置 POS 接口

POS 接口的配置主要包括：接口的链路层协议、接口时钟模式、开销字节、MTU、帧格式、加扰功能、CRC 校验功能和日志门限等方面。具体配置步骤如表 3-23 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。但在配置 POS 接口之前，需要在路由器上成功安装、注册 1STM1 或 1STM4 接口卡。

表 3-23　　POS 接口的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface pos** *interface-number* 例如：[Huawei] **interface cellular** 0/0/0	进入 POS 接口视图
3	**frame-format** { **sdh** | **sonet** } 例如：[Huawei-Pos2/0/0] **frame-format sonet**	配置 POS 接口的帧格式。由于不同的地域使用不同的同步传输体制（SDH 或 SONET），需要根据所在区域的传输体制配置 POS 接口的帧格式。命令中的选项说明如下 ● **sdh**：二选一选项，指定 POS 接口的帧格式为 SDH ● **sonet**：二选一选项，指定 POS 接口的帧格式为 SONET 缺省情况下，POS 接口的帧格式为 SDH，可用 **undo frame-format** 命令恢复为缺省设置

（续表）

步骤	命令	说明
4	**mtu** *mtu* 例如：[Huawei-Pos2/0/0] **mtu** 1200	配置 POS 接口的 MTU，不同 AR G3 路由器系列的取值范围有所不同：AR1200 系列、AR2204 和 AR2220L 为 128～1 610 的整数个字节；AR2220、AR2240 和 AR3260 为 128～1 968 整数个字节 使用本命令改变 POS 接口最大传输单元 MTU 后，需要在此接口视图下执行 **shutdown** 和 **undo shutdown** 或 **restart** 命令重启接口，以保证配置的 MTU 生效 缺省情况下，POS 接口的 MTU 值为 1 500 字节，可用 **undo mtu** 命令恢复为缺省情况
5	**link-protocol** { **fr** | **hdlc** | **ppp** } 例如：[Huawei-Pos2/0/0] **link-protocol fr**	配置 POS 接口的链路层协议，只有配置了正确的链路层协议才能配置该协议相关的参数。命令中的选项说明如下 • **fr**：多选一选项，指定 POS 接口的链路层协议为 FR（帧中继） • **hdlc**：多选一选项，指定 POS 接口的链路层协议为 HDLC（高级数据链路控制） • **ppp**：多选一选项，指定 POS 接口的链路层协议为 PPP 缺省情况下，POS 接口的链路层协议为 PPP，可用 **undo link-protocol** { **fr** | **hdlc** }命令恢复 POS 接口的链路层协议为缺省情况
6	**clock** { **master** | **slave** } 例如：[Huawei-Pos2/0/0] **clock master**	配置 POS 接口的时钟模式。POS 接口支持命令中的两个选项对应的两种时钟模式 • **master**（主时钟模式）：使用设备内部的时钟信号 • **Slave**（从时钟模式）：使用线路提供的时钟信号 【说明】当两台设备的 POS 接口直连时，应配置一端使用主时钟模式，另一端使用从时钟模式；当与 SONET/SDH 设备相连时，由于 SONET/SDH 网络的时钟精度高于 POS 本身内部时钟源的精度，应配置 POS 接口使用从时钟模式 缺省情况下，POS 接口的时钟模式为从时钟模式，可用 **undo clock** 命令恢复为缺省配置
7	**flag c2** *c2–value* **flag** { **j0** | **j1**} { **1byte-mode** *value* | **16byte-mode** *value* | **64byte-mode** *value* } 例如：[Huawei-Pos2/0/0] **flag j0 16byte-mode** aabb	配置 POS 接口的开销字节。SONET/SDH 帧具有丰富的开销字节，可完成对传输网的分层管理等运行维护功能 OAM（Operation Administration & Maintenance）。C2、J0 和 J1 字节主要用于在不同国家、不同地区或不同厂商的设备之间提供互通支持。但收发端的 C2、J0、J1 要一致，否则两端不能正常通信。这两个命令中的参数和选项说明如下 • **c2** *c2–value*：指定信号标记字节（Path signal label byte），属于高阶通道开销字节，用来指示 VC 帧的复接结构和信息净负荷的性质，16 进制形式，取值范围是 0～FF • **j0**：二选一选项，指定再生段踪迹字节（Regeneration Section Trace Message），属于再生段开销字节，用于接收端检测与发送端之间是否处于持续连接状态 • **j1**：二选一选项，指定通道踪迹字节（Higher-Order VC-N path trace byte），属于高阶通道开销字节，用于接收端与指定的发送端之间是否处于持续的连接状态 • **1byte-mode***value*：多选一参数，指定 J0/J1 的开销字节模式为 1 字节模式，参数 *value* 为 1 个字符

（续表）

步骤	命令	说明
7	**flag c2** *c2–value* **flag { j0 | j1} { 1byte-mode** *value* | **16byte-mode** *value* | **64byte-mode** *value* } 例如：[Huawei-Pos2/0/0] **flag j0 16byte-mode** aabb	• **16byte-mode** *value*：多选一参数，指定 J0/J1 的开销字节模式为 16 字节模式，参数 *value* 为 1～15 个字符 • **64byte-mode** *value*：多选一参数，指定 J0/J1 的开销字节模式为 64 字节模式，参数 *value* 为 1～62 个字符 缺省情况下，设备使用 SDH 帧格式的缺省值：开销字节 C2 的为 0x16，J0 和 J1 都为空字符串，可用 **undo flag { c2 | j0 | j1 }**命令恢复为缺省配置
8	**scramble** 例如：[Huawei-Pos2/0/0] **scramble**	配置 POS 接口对载荷数据加扰。为了避免出现过多连续的 1 或 0，便于接收端提取线路时钟信号，POS 接口支持对载荷数据的加扰功能。但要确保两端设备配置的加扰功能一致，否则会导致对接不成功 缺省情况下，POS 接口对载荷数据加扰，可用 **undo scramble** 命令禁止加扰功能
9	**crc** { **16** | **32** } 例如：[Huawei-Pos2/0/0] **crc 16**	配置 POS 接口的 CRC 校验字长度。POS 接口支持两种 CRC 校验字长度：16 bit 和 32 bit，但要保证两端设备配置的 CRC 校验字长度一致，否则会导致对接不成功。命令中的选项说明如下 • **16**：二选一选项，指定 CRC 校验字长度为 16 bit • **32**：二选一选项，指定 CRC 校验字长度为 32 bit 缺省情况下，POS 接口的 CRC 校验字长度为 32 位，可用 **undo crc** 命令恢复为缺省设置
10	**threshold** { **sd** | **sf** } *value* 例如：[Huawei-Pos2/0/0] **threshold sd 8**	配置 POS 接口日志门限。根据不同业务对链路误码率要求的不同，设置 POS 接口误码率日志门限，以便在链路性能下降时及时产生日志，网络管理员可以根据日志发现并处理链路故障，避免对业务造成影响。信号劣化（Signal Degrade，SD）和信号失效（Signal Fail，SF）日志都是用于指示当前链路性能的。它们产生的原因相同，都是接收端检测到了链路误码，当链路质量稍微下降时，产生 SD 日志，当链路质量严重下降时，产生 SF 日志。命令中的选项说明如下 • **sd** *value*：二选一选项，指定 SD（信号劣化）日志门限的指数，门限值以 10e-*value* 形式表示，*value* 为 3～9 的整数 • **sf** *value*：二选一选项，指定 SF（信号失败）日志门限的指数，门限值以 10e-*value* 形式表示，*value* 为 3～9 的整数 但配置日志 SD 门限值要比 SF 门限值小 缺省情况下，SD 门限值为 10e-6，SF 门限值为 10e-3，可用 **undo threshold** { **sd** | **sf** }命令恢复为缺省情况

3.9.3 POS 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 POS 接口，也可用以下 **reset** 用户视图命令清除 POS 接口上的统计信息（当你需要统计一定时间内 POS 接口生成的串口的流量信息时，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display interface pos** [*interface-number*]：查看所有或者指定 POS 接口配置及状态。

② **display interface brief**：查看 POS 接口的简要信息。

③ **reset counters interface** [*interface-type* [*interface-number*]]：清除所有或者指定POS接口上的统计信息。

有关POS接口的环回检测功能配置方法与3.4.6小节介绍的CE1/PRI接口的环回检测功能配置方法总体一样，只是这里要在POS接口视图下配置，参见即可。

3.9.4　POS接口物理参数配置示例

本示例基本网络结构如3-23所示，两台设备通过SONET网络相连，RouterB已经完成如下参数设置，为了保证对接成功，需要完成RouterA的POS接口配置。

① RouterB的POS接口的帧格式为SONET。

② RouterB的POS接口的链路层协议为HDLC。

③ RouterB的POS接口的时钟模式为从时钟模式。

④ RouterB的POS接口的MTU值为1 200字节。

⑤ RouterB的POS接口的对载荷数据不加扰。

⑥ RouterB的POS接口的CRC校验字长度为16位。

⑦ RouterB的POS接口的开销字节c2为3，j0和j1都按16字节模式取值，其中j0为abc、j1为xyz。



图3-23　POS接口物理参数配置示例基本网络结构

本示例的配置很简单，因为两个路由器都是直接与SONET网络相连的，所以可以直接采用SONET网络中精度更高的时钟，都采用从时钟模式。这样一来，两个路由器上的以上所有参数配置都**必须完全一致**（否则会出现物理层状态为Up，链路层状态为Down，连通不成功的现象），RouterA上的具体配置步骤如下。

① 配置RouterA的POS接口帧格式为SONET。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] frame-format sonet
```

② 配置RouterA的POS接口链路层协议为HDLC。

```
[RouterA-Pos2/0/0] link-protocol hdlc
```

③ 配置RouterA的POS接口使用从时钟模式。

```
[RouterA-Pos2/0/0] clock slave
```

④ 配置RouterA的POS接口MTU值为1 200。

```
[RouterA-Pos2/0/0] mtu 1 200
```

⑤ 配置RouterA的POS接口开销字节。

```
[RouterA-Pos2/0/0] flag c2 3
[RouterA-Pos2/0/0] flag j0 16byte-mode abc
[RouterA-Pos2/0/0] flag j1 16byte-mode xyz
```

⑥ 配置RouterA的POS接口加扰功能。

```
[RouterA-Pos2/0/0] undo scramble
```

⑦ 配置 RouterA 的 POS 接口 CRC 校验字为 16 位。

```
[RouterA-Pos2/0/0] crc 16
```

最后配置 RouterA 的 POS 接口 IP 地址。

```
[RouterA-Pos2/0/0] ip address 10.1.1.1 30
```

配置好后，可用 **display interface pos** 2/0/0 命令查看 RouterA 的 POS 接口连通状态，验证配置结果。也可以用 ping 命令验证两个路由器 POS 接口的连通性。

3.10 CPOS 接口配置与管理

CPOS 是通道化的 POS 接口，主要用于提高设备对低速接入的汇聚能力。当需要通过路由器汇聚 SONET/SDH 传输网的 E1/T1 线路时就可以使用 CPOS，可汇聚接入各个分支的 E1/T1 线路，提高了设备对低速接入的汇聚能力。在 AR G3 系列路由器中 CPOS 接口由 1CPOS-155M 或 1CPOS-155M-W 接口卡提供（图 3-24 所示的是 1CPOS-155M），**仅 AR2204、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3260 支持 CPOS 接口，且仅支持 STM-1 CPOS 接口。**

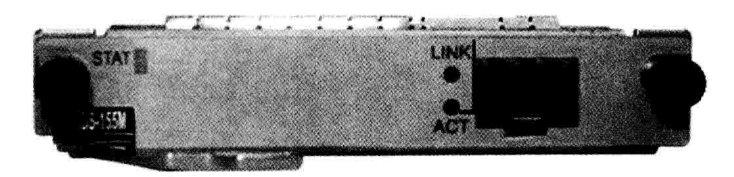


图 3-24 1CPOS-155M 接口卡

3.10.1 配置通过 CPOS 接口实现设备相连

当企业总部与区域分部间通过 CPOS 接口长距离传输数据时，可以配置 CPOS 接口之间通过光纤直接连接或通过 WDM（Wavelength Division Multiplexing 波分复用）技术相连。但在配置通过 CPOS 接口实现设备相连前，需确保 1CPOS-155M 或 1CPOS-155M-W 接口卡在路由器上成功安装、注册。

如图 3-25 所示，区域分部路由器 RouterA 与企业总部路由器 RouterB 的 CPOS 接口通过光纤直接连接或通过 WDM 相连，以便将区域分部的数据传输到总部。

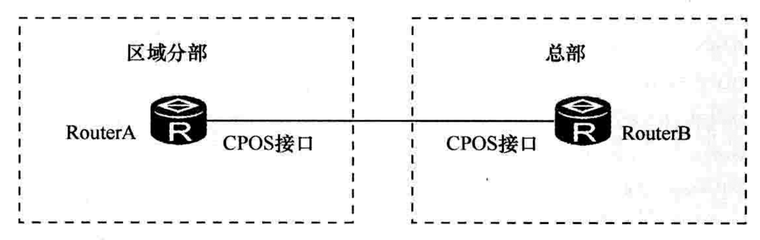


图 3-25 CPOS 接口通过光纤直接连接或通过 WDM 相连示意图

配置 CPOS 接口之间通过光纤直接相连或者 WDM 技术相连主要包括如下两项配置任务。

（1）配置 CPOS 接口之间的对接模式

当本端设备和对端设备的 CPOS 接口通过光纤直接连接或通过 WDM 相连，而对端设备为非华为技术有限公司设备时，需要配置 CPOS 接口的对接模式。但当各个分支节点的 E1/T1 链路通过 SDH/SONET 网络汇聚到路由器的 CPOS 接口时，不需要配置 CPOS 接口的对接模式。

AR G3 系列路由器提供了 3 种对接模式，分别用于与阿尔卡特设备、华为技术有限公司设备和朗讯设备对接，请根据实际情况选择对接模式。

（2）配置 CPOS 接口的线路属性

SDH 与 SONET 是两种同步传输体制，分别由不同的组织制定，两者除了在技术细节参数上有一些差别外，在实质内容和主要规范上并没有很大区别，但是两者应用的地域范围有所不同（SDH 主要应用于欧洲和中国，SONET 主要应用于北美和日本），不同设备厂商也有不同的缺省配置。

以上两项主要配置任务的具体配置步骤如表 3-24 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表 3-24　　通过光纤直接连接或通过 WDM 连接时的 CPOS 接口的配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**controller cpos** *cpos-number* 例如：[Huawei] **controller cpos** 1/0/0	进入指定 CPOS 接口的接口视图
配置CPOS接口的对接模式	3	**multi-channel align-mode** { **alcatel** | **huawei** | **lucent** } 例如：[Huawei-Cpos1/0/0] **multi-channel align-mode align-mode lucent**	配置 CPOS 接口的对接模式。命令中的选项说明如下 • **alcatel**：多选一选项，指定对接模式为阿尔卡特。当对端设备为阿尔卡特设备时，选择此模式 • **huawei**：多选一选项，指定对接模式为华为。当对端设备为华为技术有限公司设备时，选择此模式 • **lucent**：多选一选项，指定对接模式为朗讯。当对端设备为朗讯设备时，选择此模式 缺省情况下，CPOS 接口的对接模式为 huawei，即默认对端设备也为华为技术有限公司设备，可用 **undo multi-channel align-mode** 命令恢复为缺省情况
	4	**frame-format** { **sdh** | **sonet** } 例如：[Huawei-Pos2/0/0] **frame-format sonet**	配置 CPOS 接口的帧格式。由于不同的地域使用不同的同步传输体制（SDH 或 SONET），因此需要根据所在区域的传输体制配置 POS 接口的帧格式。命令中的选项说明如下 • **sdh**：二选一选项，指定 CPOS 接口的帧格式为 SDH • **sonet**：二选一选项，指定 CPOS 接口的帧格式为 SONET CPOS 接口的帧格式必须与对端设备保持一致 缺省情况下，CPOS 接口的帧格式为 SDH，可用 **undo frame-format** 命令恢复为缺省设置

（续表）

配置任务	步骤	命令	说明
配置CPOS接口的对接模式	5	**multiplex mode** { **au-4** | **au-3** } 例如：[Huawei-Cpos1/0/0] **multiplex mode au-3**	配置当 **CPOS 接口帧格式为 SDH** 时的 AUG 复用路径。命令中的选项说明如下。 ● **au-4**：二选一选项，指定 CPOS 接口的 AUG 复用路径为 AU-4 ● **au-3**：二选一选项，定 CPOS 接口的 AUG 复用路径为 AU-3 当 CPOS 接口的帧格式为 SONET 时，则只能复用到 AU-3，不能使用本命令进行配置 缺省情况下，CPOS 接口的 AUG 复用路径为 AU-4，可用 **undo multiplex mode** 命令恢复缺省设置
	6	**clock** { **master** | **slave** } 例如：[Huawei-Pos2/0/0] **clock master**	配置 CPOS 接口的时钟模式。CPOS 接口支持命令中的两个选项对应的两种时钟模式 ● **master**（主时钟模式）：使用设备内部的时钟信号 ● **Slave**（从时钟模式）：使用线路提供的时钟信号 【说明】当两台设备的 CPOS 接口直连时，应配置一端使用主时钟模式，另一端使用从时钟模式；当与SONET/SDH设备相连时，由于SONET/SDH网络的时钟精度高于 CPOS 本身内部时钟源的精度，应配置 CPOS 接口使用从时钟模式 缺省情况下，CPOS 接口的时钟模式为从时钟模式，可用 **undo clock** 命令恢复为缺省配置
	7	**flag** { **c2** *c2-value* | { **j0** | **j1** } { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* | **64byte-mode** *64byte-string* } | **s1** *s1-string* } 例如：[Huawei-Cpos1/0/0] **flag s1 10**	配置 CPOS 接口 SONET/SDH 帧的开销字节。C2、J0、J1 和 S1 字节主要用于在不同国家、不同地区或不同厂商的设备之间提供互通支持。但收发端的 C2、J0、J1 和 S1 要一致，否则两端不能正常通信。这两个命令中的参数和选项说明如下 ● **c2** *c2–value*：指定信号标记字节（Path signal label byte），属于高阶通道开销字节，用来指示 VC 帧的复接结构和信息净负荷的性质，取值范围为 0～255 的整数 ● **j0**：二选一选项，指定再生段踪迹字节（Regeneration Section Trace Message），属于再生段开销字节，用于接收端检测与发送端之间是否处于持续连接状态 ● **j1**：二选一选项，指定通道踪迹字节（Higher-Order VC-N path trace byte），属于高阶通道开销字节，用于接收端与指定的发送端之间是否处于持续的连接状态 ● **1byte-mode***value*：多选一参数，指定 J0/J1 的开销字节模式为 1 字节模式，参数 *value* 为 1 个字符 ● **16byte-mode** *value*：多选一参数，指定 J0/J1 的开销字节模式为 16 字节模式，参数 *value* 为 1～15 个字符

（续表）

配置任务	步骤	命令	说明
配置CPOS接口的对接模式	7	**flag** { **c2** *c2-value* | { **j0** | **j1** } { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* | **64byte-mode** *64byte-string* } | **s1** *s1-string* } 例如：[Huawei-Cpos1/0/0] **flag s1 10**	• **64byte-mode** *value*：多选一参数，指定 J0/J1 的开销字节模式为 64 字节模式，参数 *value* 为 1～62 个字符 • **s1** *s1-string*：多选一参数，指定同步状态字节 S1，取值范围为 0～15 的整数 缺省情况下，设备使用 SDH 帧格式的缺省值：开销字节 C2 的开销值为 2，J0 和 J1 都为空字符串，S1 为 15，可用 **undo flag** { **c2** | **j0** | **j1**| **s1** } 命令恢复为缺省配置
	8	**itf** { **number** *number* | **type** { **7e** | **ff** } } 例如：[Huawei-Cpos1/0/0] **itf type ff**	配置 CPOS 接口的帧间填充符类型和最少个数。CPOS 接口的帧间填充符是指在已经被绑定到逻辑通道的时隙在没有发送业务数据时发送的码型。CPOS 接口的帧间填充符有两种：0x7e 和 0xff。实际应用中，推荐使用缺省值，即帧间填充符类型为 0x7e。命令中的参数和选项说明如下 • **number** *number*：二选一参数，设置帧间填充符的最少个数，取值范围为 0～14 的整数 • **type** { **7e** | **ff** }：二选一选项，设置帧间填充符的类型为 0x7e 或 0xff 【说明】线路两端的帧间填充符必须配置成相同的码型和最少个数，否则可能导致通信异常。另外，由于有帧间填充符作为额外开销，CPOS 接口形成的 E1/T1 通道的实际传输速率一般达不到带宽值，为了提高 CPOS 接口实际传输速率，用户可以执行 **itf number** 命令将帧间填充符的最少个数设置为 0 缺省情况下，CPOS 接口的帧间填充符类型为 0x7e，最少个数为 4 个，可用 **undo itf** { **number** | **type** }命令恢复为缺省情况

3.10.2　配置 CPOS 接口汇聚接入 E1 线路

当企业多个分支通过 E1、T1 线路接入到 SONET/SDH 传输网时，为了节约成本、提高设备对低速接入的汇聚能力，企业区域分部可以使用 CPOS 接口汇聚接入这些 E1、T1 线路，以便实现企业区域分部与各个分支之间的数据传输。本节介绍汇聚接入 E1 线路的 CPOS 接口配置。

如图 3-26 所示，企业的几个分支使用中低端路由器通过 E1/T1 线路接入到 SONET/SDH 传输网，而企业的另外几个分支带宽需求较大，一条 E1/T1 线路满足不了需求，因此进行了扩容，同时租用几个 E1/T1 线路。所有分支经过 SONET/SDH 传输网汇聚到区域分部路由器 RouterA 上的一个或者几个 CPOS 接口，RouterA 通过时隙唯一识别各中低端路由器。这种应用在逻辑上等同于各中低端路由器分别通过 E1/T1 或者 N×E1/T1 的线路接入 RouterA。

实际情况中，CPOS 接口与各中低端路由器之间可能经过不止一级 SONET/SDH 传

输网，各中低端路由器与 SONET/SDH 传输网之间可能还需要其他的传输手段进行中继。CPOS 接口可以通道化形成多个 E1/T1 通道，以便汇聚来自不同企业分支的 E1/T1 线路。其中，每个 E1/T1 线路可以包含一个通道，也可以包含多个通道。

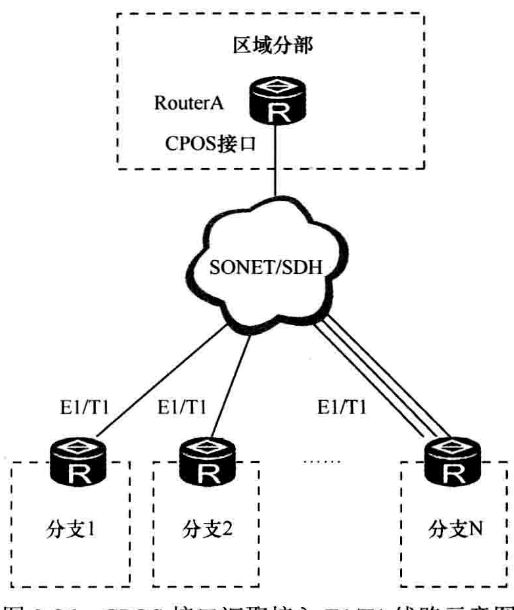


图 3-26 CPOS 接口汇聚接入 E1/T1 线路示意图

CPOS 接口形成 E1 通道有两种工作模式：非通道化模式和通道化模式。

① 当 E1 通道工作在非通道模式时，它相当于一个不分时隙、数据带宽为 2.048 Mbit/s 的接口，其逻辑特性与同步串口相同。

② 当 E1 通道工作在通道化模式时，2 Mbit/s 的传输线路分成了 32 个 64 kbit/s 的时隙，对应编号为 0～31，其中 0 时隙用于传输同步信息。除 0 时隙外的全部时隙任意分成一个组（channel set），这个组作为一个接口使用，其速率为 N×64 kbit/s，逻辑特性与同步串口相同。

在配置 CPOS 接口汇聚接入 E1 线路前，需要确保 1CPOS-155M 或 1CPOS-155M-W 接口卡在路由器上成功安装、注册；确保 SDH 传输设备的各级复用单元配置与设备 CPOS 的 E1 通道序号对应正确。主要包括以下两项配置任务：一是配置 CPOS 接口的线路属性，二是配置 CPOS 接口下的 E1 通道。具体配置步骤如表 3-25 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。总体与 3.10.2 小节表 3-24 中介绍的通过光纤直接连接或通过 WDM 连接的 CPOS 接口配置类似。

表 3-25 CPOS 接口汇聚接入 E1 线路的配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**controller cpos** *cpos-number* 例如：[Huawei] **controller cpos** 1/0/0	进入指定 CPOS 接口的接口视图
配置 CPOS 接口的线路属性	3	**frame-format** { **sdh** | **sonet** } 例如：[Huawei-Pos2/0/0] **frame-format sonet**	配置 CPOS 接口的帧格式。其他说明参见上节表 3-24 第 4 步说明
	4	**multiplex mode** { **au-4** | **au-3** } 例如：[Huawei-Cpos1/0/0] **multiplex mode au-3**	配置当 **CPOS 接口帧格式为 SDH 时**的 AUG 复用路径。其他说明参见上节表 3-24 第 5 步说明
	5	**clock** { **master** | **slave** } 例如：[Huawei-Cpos1/0/0] **clock master**	配置 CPOS 接口的时钟模式。其他说明参见上节表 3-24 第 6 步说明
	6	**quit** 例如：[Huawei-Cpos1/0/0] **quit**	退出 CPOS 接口视图，返回系统视图

（续表）

配置任务	步骤	命令	说明
配置CPOS接口下的E1通道	7	**set workmode slot** *slot-id* **cpos e1-data** 例如：[Huawei] **set workmode slot** 1 **cpos e1-data**	配置 CPOS 接口卡工作在 E1 模式下，参数 *slot-id* 用来指定需要更改工作模式的接口卡所在的槽位号。可先使用 **display device** 命令查看设备上的接口卡槽位号及类型，再找出单板类型带有"1CPOS-155M"的单板槽位号，也可使用 **display workmode** 命令 1CPOS-155M 接口卡的工作模式为 e1-data 的板槽位号 执行该步骤后，需要重启单板并等待一段时间才能使配置生效 缺省情况下，CPOS 接口卡的工作模式为 e1-data，即 E1 模式
	8	**controller cpos** *cpos-number* 例如：[Huawei] **controller cpos** 1/0/0	进入指定 CPOS 接口的接口视图
	9	**e1** *e1-number* **unframed** 例如：[Huawei-Cpos1/0/0] **e1** 3 **unframed**	（二选一）配置 E1 通道工作在非通道化模式。参数 *e1-number* 用来指定 CPOS 接口的 E1 通道号，取值范围为 1～63 的整数 配置完成后，设备将生成一个不分时隙、数据带宽为 2.048 Mbit/s 的逻辑通道。用户可通过执行命令 **interface serial** *cpos-number*/*e1-number*:**0** 访问该逻辑通道，其中，*interface-number* 是 CPOS 的接口编号，*e1-number* 是 E1 通道的编号 缺省情况下，E1 通道工作在通道化模式，可用 **undo e1** *e1-number* **unframed** 命令恢复指定 E1 通道为缺省情况 **在非通道模式和通道化模式之间切换前，需要先删除原先的工作模式的配置**
		e1 *e1-number* **channel-set** *set-number* **timeslot-list** *slot-list* 例如：[Huawei-Cpos1/0/0] **e1 63 channel-set** 1 **timeslot-list** 1-31	（二选一）配置 E1 通道工作在通道化模式，并对 E1 通道进行时隙捆绑。命令中的参数说明如下 • *e1-number*：指定 CPOS 接口的 E1 通道号，取值范围为 1～63 的整数 • *set-number*：指定捆绑集的编号，取值范围为 0～30 的整数 • *slot-list*：指定用于捆绑的时隙编号或时隙范围，取值范围为 0～31 的整数，指定捆绑时隙时，可以指定单个时隙，也可以指定时隙范围，包括使用","分隔多个时隙以及使用"-"表示时隙范围 配置完成后，设备将生成一个由时隙 *slot-list* 组成、速率为 *N*×64 kbit/s（*N* 为捆绑的时隙数）的逻辑通道。用户可通过执行命令 **interface serial** *cpos-number*/*e1-number*:*set-number* 访问该逻辑通道，其中，*interface-number* 是 CPOS 的接口编号，*e1-number* 是 E1 通道编号，*set-number* 是时隙捆绑的捆绑集编号

（续表）

配置任务	步骤	命令	说明
配置CPOS接口下的E1通道	9	**e1** *e1-number* **channel-set** *set-number* **timeslot-list** *slot-list* 例如：[Huawei-Cpos1/0/0] **e1 63 channel-set** 1 **timeslot-list** 1-31	缺省情况下，设备不对E1通道进行时隙捆绑，可用 **undo e1** *e1-number* **channel-set** *set-number* 命令取消指定的时隙捆绑 在非通道模式和通道化模式之间切换前，需要先删除原先的工作模式的配置
	10	**e1** *e1-number* **set frame-format** { **crc4** | **no-crc4** } 例如：[Huawei-Cpos1/0/0] **e1** 1 **set frame-format crc4**	配置**在成帧模式下（非成帧模式下不能使用本命令）**E1通道的帧格式。命令中的参数和选项说明如下 ● *e1-number*：指定CPOS接口的E1通道号，取值范围为1～63的整数 ● **crc4**：二选一选项，指定E1通道的帧格式为CRC4帧格式 ● **no-crc4**：二选一选项，指定E1通道的帧格式为非CRC4帧格式 E1通道的帧格式必须与对端设备E1线路的帧格式保持一致 缺省情况下，E1通道的帧格式为非CRC4帧格式，可用 **undo e1** *e1-number* **set frame-format** 命令恢复指定E1通道的帧格式为缺省情况
	11	**e1** *e1-number* **set flag** { **j2** { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* } | **v5** *v5-string* } 例如：[Huawei-Cpos1/0/0] **e1** 1 **set flag v5** 2	配置E1通道的通道开销。命令中的参数和选项说明如下 ● *e1-number*：指定CPOS接口的E1通道号，取值范围为1～63的整数 ● **j2 1byte-mode** *1byte-string*：多选一参数，指定低阶通道踪迹字节J2的开销字节模式为1字节模式，为1个字符 ● **j2 16byte-mode** *16byte-string*：多选一参数，指定低阶通道踪迹字节J2的开销字节模式为16字节模式，为1～15个字符 ● **v5** *v5-string*：多选一参数，指定低阶通道信号标签字节V5，取值范围为0～5的整数。E1模式下，V5只能取1、3和5，缺省值是1 建议E1通道的通道开销与对端设备E1线路的通道开销保持一致，否则可能会造成通信异常 缺省情况下，J2为空字符串，V5取值为1，可用 **undo e1** *e1-number* **set flag** { **j2** | **v5** }命令恢复为缺省情况
	12	**e1** *e1-number* **set clock** { **master** | **slave** } 例如：[Huawei-Cpos1/0/0] **e1** 1 **set clock master**	配置E1通道的时钟模式。命令中的参数和选项说明如下 ● *e1-number*：指定CPOS接口的E1通道号，取值范围为1～63的整数 ● **master**：二选一选项，指定时钟模式为主时钟模式 ● **slave**：二选一选项，指定时钟模式为从时钟模式 同一个CPOS接口的不同E1通道的时钟模式是相互独立的，而且**E1通道的时钟模式必须与对端设备E1线路的时钟模式不同** 缺省情况下，E1通道的时钟模式为从时钟（slave），可用 **undo e1** *e1-number* **set clock** 命令恢复为缺省情况

（续表）

配置任务	步骤	命令	说明
配置 CPOS 接口下的 E1 通道	13	**e1** *e1-number* **shutdown** 例如：[Huawei-Cpos1/0/0] **e1** 1 **shutdown** 或 **undo e1** *e1-number* **shutdown** 例如：[Huawei-Cpos1/0/0] **undo e1** 1 **shutdown**	关闭或启动指定 E1 通道，参数 *e1-number* 用来指定要关闭或者启动的 CPOS 接口的 E1 通道号 缺省情况下，E1 通道是启动的

3.10.3　配置 CPOS 接口汇聚接入 T1 线路

当企业多个分支通过 T1 线路接入到 SONET/SDH 传输网时，为了节约成本、提高设备对低速接入的汇聚能力，企业区域分部可以使用 CPOS 接口汇聚接入这些 T1 线路，以便实现企业区域分部与各个分支之间的数据传输。北美和日本广泛应用 T1 系统。

CPOS 接口形成 T1 通道有两种工作模式：非通道化模式和通道化模式。

① 当 T1 通道工作在非通道化模式时，相当于一个不分时隙、数据带宽为 1.544 Mbit/s 的接口，其逻辑特性与同步串口相同。

② 当 T1 通道工作在通道化模式时，其全部时隙（时隙 1～24）可以任意地分成一个组，这个组作为一个接口使用，其速率为 N×56 kbit/s 或 N×64 kbit/s，逻辑特性与同步串口相同。

缺省情况下，T1 通道工作在通道化模式。

在配置 CPOS 接口汇聚接入 T1 线路前，需要确保 1CPOS-155M 或 1CPOS-155M-W 接口卡在路由器上成功安装、注册，确保 SDH 传输设备的各级复用单元配置与设备 CPOS 的 T1 通道序号对应正确。主要包括以下两项配置任务：一是配置 CPOS 接口的线路属性，二是配置 CPOS 接口下的 T1 通道。具体配置步骤如表 3-26 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。总体与上节介绍的接入 E1 线路的配置类似，主要区别就在于用到的线路不同，所以其用到的命令关键词作了对应修改（由原来的 **e1** 改为 **t1**）。

表 3-26　CPOS 接口汇聚接入 T1 线路的配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**controller cpos** *cpos-number* 例如：[Huawei] **controller cpos** 1/0/0	进入指定 CPOS 接口的接口视图
配置 CPOS 接口的线路属性	3	**frame-format** { **sdh** | **sonet** } 例如：[Huawei-Pos2/0/0] **frame-format sonet**	配置 CPOS 接口的帧格式。其他说明参见 3.10.1 小节表 3-24 第 4 步说明

（续表）

配置任务	步骤	命令	说明
配置 CPOS 接口的线路属性	4	**multiplex mode** { **au-4** | **au-3** } 例如：[Huawei-Cpos1/0/0] **multiplex mode au-3**	配置当 **CPOS 接口帧格式为 SDH** 时的 AUG 复用路径。其他说明参见 3.10.1 小节表 3-24 第 5 步说明
	5	**clock** { **master** | **slave** } 例如：[Huawei-Cpos1/0/0] **clock master**	配置 CPOS 接口的时钟模式。其他说明参见 3.10.1 小节表 3-24 第 6 步说明
	6	**quit** 例如：[Huawei-Cpos1/0/0] **quit**	退出 CPOS 接口视图，返回系统视图
配置 CPOS 接口下的 E1 通道	7	**set workmode slot** *slot-id* **cpos e1-data** 例如：[Huawei] **set workmode slot** 1 **cpos t1-data**	配置 1CPOS-155M 接口卡工作在 E1 模式下，参数用来指定需要更改工作模式的接口卡所在的槽位号。可先使用 **display device** 命令查看设备上的接口卡槽位号及类型，再找出单板类型带有“1CPOS-155M”的单板槽位号，也可使用 **display workmode** 命令 1CPOS-155M 接口卡的工作模式为 t1-data 的板槽位号 执行该步骤后，需要重启单板并等待一段时间才能使配置生效 缺省情况下，1CPOS-155M 接口卡的工作模式为 e1-data，即 E1 模式
	8	**controller cpos** *cpos-number* 例如：[Huawei] **controller cpos** 1/0/0	进入指定 CPOS 接口的接口视图
	9	**t1** *t1-number* **unframed** 例如：[Huawei-Cpos1/0/0] **t1** 3 **unframed**	（二选一）配置 T1 通道工作在非通道化模式。参数 *t1-number* 用来指定 CPOS 接口的 T1 通道号，取值范围为 1～84 的整数 配置完成后，设备将生成一个不分时隙、数据带宽为 1.544 Mbit/s 的逻辑通道。用户可通过执行命令 **interface serial** *cpos-number*/*t1-number*：**0** 访问该逻辑通道，其中，*interface-number* 是 CPOS 的接口编号，*t1-number* 是 T1 通道的编号 缺省情况下，T1 通道工作在通道化模式，可用 **undo e1** *t1-number* **unframed** 命令恢复指定 T1 通道为缺省情况 在非通道模式和通道化模式之间切换前，需要先删除原先的工作模式的配置
		t1 *e1-number* **channel-set** *set-number* **timeslot-list** *slot-list* [**speed** {**56k** | **64k** }] 例如：[Huawei-Cpos1/0/0] **t1 63 channel-set** 1 **timeslot- list** 1-24 **speed 64k**	（二选一）配置 T1 通道工作在通道化模式，并对 T1 通道进行时隙捆绑。命令中的参数说明如下 ● *t1-number*：指定 CPOS 接口的 E1 通道号，取值范围为 1～84 的整数 ● *set-number*：指定捆绑集的编号，取值范围为 0～23 的整数 ● *slot-list*：指定用于捆绑的时隙编号或时隙范围，取值范围为 0～24 的整数，指定捆绑时隙时，可以指定单个时隙，也可以指定时隙范围，包括使用“,”分隔多个时隙以及使用“-”表示时隙范围

（续表）

配置任务	步骤	命令	说明
配置 CPOS 接口下的 E1 通道	9	**t1** *e1-number* **channel-set** *set-number* **timeslot-list** *slot-list* [**speed** {**56k** | **64k** }] 例如：[Huawei-Cpos1/0/0] **t1 63 channel-set** 1 **timeslot- list** 1-24 **speed 64k**	• **speed** {**56k** | **64k** }：可选项，指定时隙捆绑的方式：选用 56 k 选项时，捆绑方式为 *N*×56 kbit/s；选用 64k 选项时，捆绑方式为 *N*×64 kbit/s；如果不指定速率，缺省采用 *N*×64 kbit/s 配置完成后，设备将生成一个由时隙 *slot-list* 组成、速率为 *N*×56 kbit/s 或 *N*×64 kbit/s（*N* 为捆绑的时隙数）的逻辑通道。用户可通过执行命令 **interface serial** *cpos-number*/*t1-number*：*set-number* 访问该逻辑通道，其中，*interface-number* 是 CPOS 的接口编号，*t1- number* 是 E1 通道编号，*set-number* 是时隙捆绑的捆绑集编号 缺省情况下，设备不对 T1 通道进行时隙捆绑，可用 **undo e1** *t1-number* **channel-set** *set-number* 命令取消指定的时隙捆绑 在非通道化模式和通道化模式之间切换前，需要先删除原先的工作模式的配置
	10	**t1** *t1-number* **set frame-format** { **esf** | **sf** } 例如：[Huawei-Cpos1/0/0] **t1** 1 **set frame-format esf**	**配置在成帧模式下（非成帧模式下不能使用本命令）**的 T1 通道的帧格式。命令中的参数和选项说明如下 • *t1-number*：指定 CPOS 接口的 T1 通道号，取值范围为 1～84 的整数 • **esf**：二选一选项，指定 11 通道的帧格式为 ESF 格式。ESF 帧是由 24 帧组成多帧，共享相同的帧同步信息和信令信息的扩展超帧技术，其中帧 6、12、18、24 共四个信令帧 • **sf**：二选一选项，指定 T1 通道的帧格式为 SF 格式。SF 帧是由 12 帧组成多帧，共享相同的帧同步信息和信令信息的超帧技术，其中帧 6 和 12 共两个信令帧 T1 通道的帧格式必须与对端设备 T1 线路的帧格式保持一致 缺省情况下，T1 通道的帧格式为 ESF 帧格式，可用 **undo t1** *t1-number* **set frame-format** 命令恢复指定 T1 通道的帧格式为缺省情况
	11	**t1** *t1-number* **set flag** { **j2** { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* } | **v5** *v5-string* } 例如：[Huawei-Cpos1/0/0] **t1** 1 **set flag v5** 2	配置 T1 通道的通道开销。命令中的参数和选项说明如下 • *t1-number*：指定 CPOS 接口的 T1 通道号，取值范围为 1～84 的整数 • **j2 1byte-mode** *1byte-string*：多选一参数，指定低阶通道踪迹字节 J2 的开销字节模式为 1 字节模式，为 1 个字符 • **j2 16byte-mode** *16byte-string*：多选一参数，指定低阶通道踪迹字节 J2 的开销字节模式为 16 字节模式，为 1～15 个字符 • **v5** *v5-string*：多选一参数，指定低阶通道信号标签字节 V5，取值范围为 0～5 的整数。E1 模式下，V5 只能取 0、2 和 4，缺省值是 0 建议 T1 通道的通道开销与对端设备 T1 线路的通道开销保持一致，否则可能会造成通信异常 缺省情况下，J2 为空字符串，V5 取值为 0，可用 **undo t1** *t1-number* **set flag** { **j2** | **v5** }命令恢复为缺省情况

（续表）

配置任务	步骤	命令	说明
配置CPOS接口下的E1通道	12	**t1** *e1-number* **set clock** { **master** | **slave** } 例如：[Huawei-Cpos1/0/0] **t1** 1 **set clock master**	配置 T1 通道的时钟模式。命令中的参数和选项说明如下 ● *e1-number*：指定 CPOS 接口的 T1 通道号，取值范围为 1～84 的整数 ● **master**：二选一选项，指定 E1 通道的时钟模式为主时钟模式 ● **slave**：二选一选项，指定 E1 通道的时钟模式为从时钟模式 同一个 CPOS 接口的不同 T1 通道的时钟模式是相互独立的，而且 **T1 通道的时钟模式必须与对端设备 E1 线路的时钟模式不同** 缺省情况下，T1 通道的时钟模式为从时钟（slave），可用 **undo t1** *t1-number* **set clock** 命令恢复为缺省情况
	13	**t1** *e1-number* **shutdown** 例如：[Huawei-Cpos1/0/0] **t1** 1 **shutdown** 或 **undo t1** *e1-number* **shutdown** 例如：[Huawei-Cpos1/0/0] **undo t1** 1 **shutdown**	关闭或启动指定 T1 通道，参数 *e1-number* 用来指定要关闭或者启动的 CPOS 接口的 T1 通道号 缺省情况下，T1 通道是启动的

3.10.4 CPOS 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 CPOS 接口，也可用以下 **reset** 用户视图命令清除 CPOS 接口上的统计信息（当你需要统计一定时间内 CPOS 接口生成的串口的流量信息时，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display controller cpos** [*cpos-number*]：查看 CPOS 接口配置及其所有 E1/T1 通道的物理层配置信息状态。

② **display controller cpos** *cpos-number* **e1** *t1-number*：查看指定 CPOS 接口的指定 E1 通道的物理层配置信息。

③ **display controller cpos** *cpos-number* **t1** *t1-number*：查看指定 CPOS 接口的指定 T1 通道的物理层配置信息。

④ **reset counters interface** [*interface-type* [*interface-number*]]：清除 CPOS 接口或 CPOS 接口形成的 E1/T1 通道的统计信息。

POS 接口的环回检测功能配置的方法是在 POS 接口视图下根据实际的接口类型选择配置。

① 如果是检测 CPOS 接口，执行 **loopback** { **local** | **remote** }命令。

② 如果是检测 CPOS 接口下的 E1 通道，执行 **e1** *e1-number* **set loopback** { **local** | **remote** }命令，参数 *e1-number* 用来指定要配置环回检测功能的 E1 通道编号，取值范围为 1～63 的整数。

③ 如果是检测 CPOS 接口下的 T1 通道，执行 **t1** *t1-number* **set loopback** { **local** |

remote }命令，参数 *t1-number* 用来指定要配置环回检测功能的 T1 通道编号，取值范围为 1～84 的整数。

缺省情况下，禁止接口的环回检测功能。

3.10.5　CPOS 接口通过光纤直连的配置示例

如图 3-27 所示，RouterA 和 RouterB 的 CPOS 接口通过光纤直接相连。现已知如下条件。

① RouterA 和 RouterB 所在区域使用 SDH 传输体制。

② RouterA 和 RouterB 所在区域的 AUG 复用路径为 AU-3 复用。

③ RouterB 为阿尔卡特设备。

④ RouterB 的 CPOS 接口的时钟模式为从时钟模式。

⑤ RouterB 的 CPOS 接口开销字节 c2 为 3、s1 为 14，j0 和 j1 都按 16 字节模式取值，其中 j0 为 abc、j1 为 xyz。

为了保证对接成功，需要完成 RouterA 的 CPOS 接口配置。

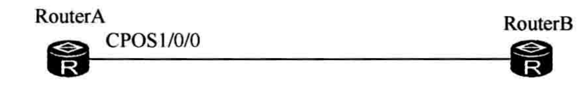


图 3-27　CPOS 接口通过光纤直连的配置示例基本网络结构

根据本示例的已知条件以及 3.10.2 小节介绍的配置方法可以得出本示例的配置思路如下（除时钟模式配置外，其他配置必须与 RouterB 上的配置一致）。

① 配置 RouterA 的对接模式为 alcatel。

② 配置 RouterA 的 CPOS 接口的帧格式为 SDH。

③ 配置 RouterA 的 CPOS 接口的 AUG 复用路径为 AU-3 复用。

④ 配置 RouterA 的 CPOS 接口开销字节 c2 为 3、s1 为 14，j0 和 j1 都按 16 字节模式取值，其中 j0 为 abc、j1 为 xyz，以保证两端设备的开销字节一致。

⑤ 配置 RouterA 的 CPOS 接口的时钟模式为主时钟模式，以保证两端设备的时钟模式不同。

具体配置步骤如下。

① 配置 RouterA 的对接模式为 alcatel。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface cpos 1/0/0
[RouterA-Cpos1/0/0] multi-channel align-mode alcatel
```

② 配置 RouterA 的 CPOS 接口帧格式为 SDH。

```
[RouterA-Cpos1/0/0] frame-format sdh
```

③ 配置 RouterA 的 CPOS 接口的 AUG 复用路径为 AU-3 复用。

```
[RouterA-Cpos1/0/0] multiplex mode au-3
```

④ 配置 RouterA 的 POS 接口开销字节。

```
[RouterA-Cpos1/0/0] flag c2 3
[RouterA-Cpos1/0/0] flag s1 14
[RouterA-Cpos1/0/0] flag j0 16byte-mode abc
[RouterA-Cpos1/0/0] flag j1 16byte-mode xyz
```

⑤ 配置 RouterA 的 CPOS 接口的时钟模式为主时钟模式。

```
[RouterA-Cpos1/0/0] clock master
[RouterA-Cpos1/0/0] quit
```

3.10.6 CPOS 接口汇聚接入 E1 线路的配置示例

本示例网络结构如图 3-28 所示，RouterA 节点下属有 RouterB～H 7 个分支节点，每个分支节点设备通过 E1 线路上行连接到 RouterA，RouterA 通过 CPOS 接口汇聚上行的 E1 线路。

由于 RouterB 分支节点进行了扩容后，一条 E1 线路满足不了需求，因此添加了一条 E1 线路。要求用 MP-group 接口的方式，对这两条 E1 线路进行捆绑。现已知如下条件。

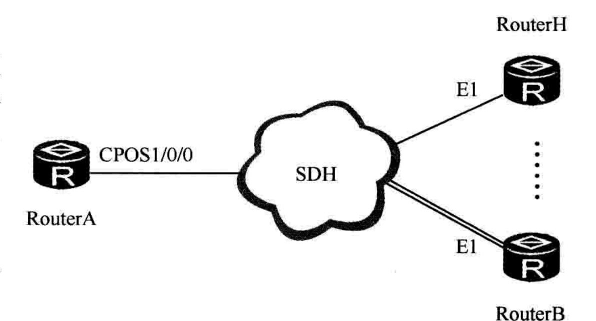


图 3-28 CPOS 接口汇聚接入 E1 线路的配置示例基本网络结构

① RouterA 使用来自 SDH 网络的时钟。

② RouterA 的 CPOS 接口的帧格式是 SDH，AUG 复用路径为 au-4。

根本示例的已知条件和要求以及 3.10.3 小节介绍的配置方法可以得出本示例的配置思路如下。

① 在 RouterA 上配置 CPOS 接口的线路属性，包括时钟模式、帧格式和 AUG 复用路径。

缺省情况下，CPOS 接口的时钟模式为从时钟模式、帧格式为 SDH 以及 AUG 复用路径为 au-4，因此本例不需要配置 CPOS 接口的线路属性。

② 分别在 RouterA 和 RouterB 上创建并配置 MP-Group。

③ 在 RouterA 上配置 CPOS 接口下的 E1 通道，并将 E1 通道进行 MP 绑定。

④ 在 RouterB 上将 E1-F 接口进行 MP 绑定。

具体的配置步骤如下。

① 在 RouterA 上创建并配置 MP-Group。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface mp-group 0/0/1
[RouterA-Mp-group0/0/1] ip address 100.10.10.1 24
[RouterA-Mp-group0/0/1] quit
```

② 配置 CPOS 接口下的两条 E1 通道。

```
[RouterA] controller cpos 1/0/0
[RouterA-Cpos1/0/0] e1 1 unframed
[RouterA-Cpos1/0/0] e1 1 set clock master
[RouterA-Cpos1/0/0] e1 2 unframed
[RouterA-Cpos1/0/0] e1 2 set clock master
[RouterA-Cpos1/0/0] quit
```

③ 将 CPOS 接口形成两条 E1 通道进行对应的 MP 绑定。

```
[RouterA] interface serial 1/0/0/1:0
[RouterA-Serial1/0/0/1:0] ppp mp mp-group 0/0/1
```

```
[RouterA-Serial1/0/0/1:0] quit
[RouterA] interface serial 1/0/0/2:0
[RouterA-Serial1/0/0/2:0] ppp mp mp-group 0/0/1
[RouterA-Serial1/0/0/2:0] quit
```

④ 在 RouterB 上创建并配置 MP-Group。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface mp-group 0/0/1
[RouterB-Mp-group0/0/1] ip address 100.10.10.2 24
[RouterB-Mp-group0/0/1] quit
```

⑤ 将 RouterB 上的 E1-F 接口进行 MP 绑定。

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] fe1 unframed
[RouterB-Serial1/0/0] ppp mp mp-group 0/0/1
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 2/0/0
[RouterB-Serial2/0/0] fe1 unframed
[RouterB-Serial2/0/0] ppp mp mp-group 0/0/1
[RouterB-Serial2/0/0] quit
```

3.11　PON 接口配置与管理

PON（Passive Optical Network，无源光网络）技术是最近发展的点到多点的光纤接入技术，是一种纯介质网络，利用光纤实现数据、语音和视频的全业务接入。PON 接口包括 EPON 接口和 GPON 接口，可以提供高速率的数据传输。在 AR G3 系列路由器中，PON 接口是由 1PON 接口卡提供的（如图 3-29 所示），**仅 AR1200 系列、AR1220-S、AR2204、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3260 支持配置 PON 接口。**

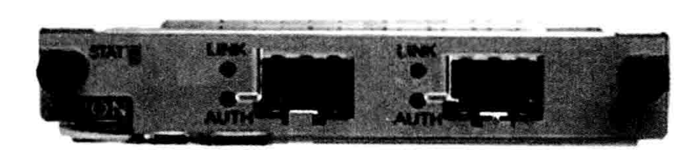


图 3-29　1PON 接口卡

3.11.1　PON 概述

PON 网络不包含任何有源电子器件，全部由无源光器件组成，避免了外部设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，简化了供电配置和网管复杂度，提高了系统可靠性，同时节省了维护成本。PON 网络的业务透明性较好，原则上可适用于任何制式和速率的信号。近年来，PON 承载由于其具备长距离传输、高 QoS 保证和高带宽性能等优势，已经逐渐成为下一代接入网的主流承载技术。

1．PON 系统组成

PON 系统由三部分组成，分别为 OLT（Optical Line Terminal，光线路终端）、ODN（Optical Distribution Network，无源光分路器）和 ONU（Optical Network Unit，光网络单

元），如图 3-30 所示。OLT 是放置在局端的终结 PON 协议的汇聚设备；ODN 是一个连接 OLT 和 ONU 的无源设备，它的功能是分发下行数据，并集中上行数据；ONU 是位于客户侧的给用户提供各种接口的用户侧终端。此处讲的 AR G3 系列路由器是作为 ONU 来部署的。

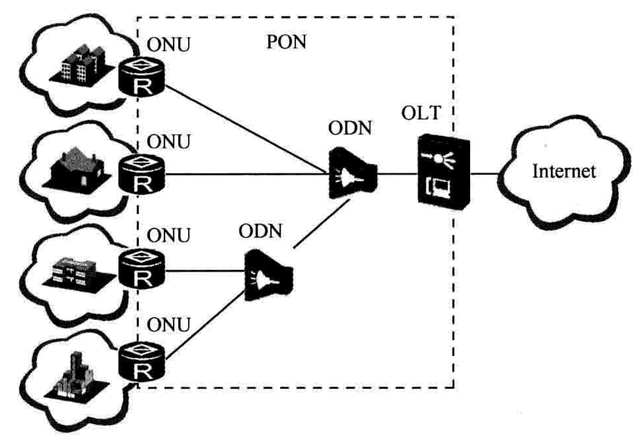


图 3-30 PON 系统典型结构

2. 上下行原理

在 PON 系统中，OLT 到 ONU 的数据传输方向称之为下行方向，反之为上行方向。AR G3 系列路由器上的 PON 接口称为 PON 上行接口。上下行方向数据传输原理是不同的。

① 下行方向：OLT 采用广播方式，将 IP 数据、语音、视频等多种业务，通过 1:N 无源光分路器分配到所有 ONU 单元。当数据信号到达 ONU 时，ONU 根据 OLT 分配的逻辑标识，在物理层上做判断，接收给它自己的数据帧，丢弃那些给其他 ONU 的数据帧。

② 上行方向：来自各个 ONU 的多种业务信息，采用 TDMA（Time Division Multiple Access，时分多址接入）技术，分时隙互不干扰地通过 1:N 无源光分路器耦合到同一根光纤，最终送到 OLT。

3. EPON 和 GPON

目前主要的 PON 技术有 EPON、GPON 两种，它们的技术标准分别由 IEEE 802.3ah 工作组和 ITU/FSAN 制定。

EPON 是基于以太网的无源光网络，是由 2000 年 11 月成立的 EFM（Ethernet in the First Mile，第一英里以太网）工作组提出的，并在 IEEE 802.3ah 标准中进行规范。它将以太网技术与 PON 技术结合起来，可提供上下行对称的 1.25 Gbit/s 线路传输速率，实现一点到多点结构的吉比特以太网光纤接入系统。

在 EFM 提出 EPON 概念的同时，ITU/FSAN 又提出了 GPON，并对其进行了标准化。GPON 的技术特色是在二层采用 ITU-T 定义的 GFP（Generic Framing Procedure，通用成帧规程）对以太网、TDM、ATM 等多种业务进行封装映射，提供 1.25 Gbit/s 和 2.5 Gbit/s 两种下行速率以及 155 Mbit/s、622 Mbit/s、1.25 Gbit/s、2.5 Gbit/s 几种上行速率，并具有较强的 OAM（操作、管理和维护）功能。在高速率和支持多业务方面，GPON 有优势，但技术的复杂和成本目前要高于 EPON，产品的成熟性也逊于 EPON。它们之间的主要特性比较如表 3-27 所示。

表 3-27　　**EPON 和 GPON 的主要特性比较**

项目	EPON	GPON
下行速率	1.25 Gbit/s	1.25 Gbit/s 或 2.5 Gbit/s
上行速率	1.25 Gbit/s	155 Mbit/s、622 Mbit/s、1.25 Gbit/s 或 2.5 Gbit/s
分路比	取决于光功率预算	取决于光功率预算
最大传输距离	10 km 或 20 km	20 km
数据链路层协议	以太网	GEM 或 ATM
封装效率	高	最高
技术标准化程度	完备	一般
芯片、器件成熟程度	高	一般
理论成本	低	低
实际成本	低	高

3.11.2　配置 EPON 接口

通过配置 EPON 接口可使路由器与上行 OLT 设备完成对接。但在配置 EPON 接口之前，需要在路由器上成功安装、注册 PON 接口卡。

EPON 接口的配置任务主要包括以下三个方面。

（1）配置工作模式

为了实现设备与支持 EPON 模式的 OLT 的顺利对接，用户可以选择设备工作在自适应模式下，也可以通过 **port mode epon** PON 接口命令手动配置设备的 PON 接口使其工作在 EPON 模式下。当 PON 接口上配有业务时，切换模式会导致业务中断，需谨慎操作。

推荐使用自适应模式，但是在自适应模式下只能自适应成功一次。例如，设备的 PON 接口已经成功自适应为 EPON 模式，当再次接入到 OLT 的 PON 接口下时，如果 OLT 的 PON 接口工作在 GPON 模式下，只有重启 PON 单板才能自适应成功。

（2）配置 ONU 认证参数

OLT 需要对 ONU 的有效性和合法性进行认证，以防非法 ONU 接入。EPON 系统支持表 3-28 所列的三种 ONU 认证方式。

表 3-28　　**EPON 系统支持的三种 ONU 认证方式及比较**

ONU 认证方式	说明	优点	缺点	应用场景
物理标识认证	采用 ONU 的物理标识（ONU 的 MAC 地址）作为标识的认证方法	配置简单，可靠性高。基于 MAC 认证通过后，禁止用户更改 MAC 地址	当 ONU 损坏需要更换新 ONU 时，新的 MAC 地址必须在 OLT 上重新添加	适用于安全需求比较高的场景
逻辑标识认证	逻辑标识包括 LOID（Logical ONU ID，逻辑 ONU ID）和 Checkcode。进行认证时有两种处理方式：仅判断 LOID 或同时判断 LOID 和 Checkcode，可灵活配置	用户在变换物理位置时，不需要重新配置逻辑标识，且提供两种处理方式，提高了终端用户接入的灵活性	若非法 ONU 盗取了合法 ONU 的逻辑标识，OLT 进行认证时，最先通过认证 ONU 的业务先上线，可能会导致合法 ONU 无法正常上线	适用于移动性需求比较高的场景

（续表）

ONU 认证方式	说明	优点	缺点	应用场景
密码认证	华为技术有限公司私有认证方式，对接的 OLT 设备也需为华为技术有限公司设备	配置简单，用户在变换物理位置时，不需要重新配置密码	对接的 OLT 需支持密码认证方式。对接的 OLT 设备也需为华为技术有限公司设备	适用于移动性需求比较高的场景

这三种认证方式可单独使用，也可组合使用。但是，在 ONU 上配置的认证参数由 OLT 预先分配，用户无法任意配置，否则认证将无法通过。因此，用户可根据 OLT 实际的认证方式配置 ONU 上的认证参数。

（3）（可选）配置光模块参数

主要可配置的 EPON 接口光模块参数包括光模块的发光模式、光模块偏置电流告警低门限和高门限值、光模块发送光功率告警低门限和高门限值、光模块温度告警低门限和高门限值、光模块电压告警低门限和高门限值。

以上三项配置任务的具体配置步骤如表 3-29 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表 3-29 EPON 接口配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**interface pon** *interface-number* 例如：[Huawei] **interface pon 1/0/0**	进入 PON 接口视图
配置工作模式	3	**port mode epon** 例如：[Huawei-Pon1/0/0] **port mode gpon**	配置当前 PON 接口工作模式为 EPON 模式。 缺省情况下，PON 接口的工作模式为自适应模式，在自适应模式下，设备会根据接入的光信号自动适应成 EPON 或者 GPON，具备较强的适应性，推荐使用自适应模式 【注意】**port mode** 命令的执行结果是覆盖式的，即如果两次配置的工作模式不同，则第二次的配置生效。但 PON 接口不支持 EPON 模式和 GPON 模式之间直接切换，用户必须先将 PON 接口切换到自适应模式，才能进一步切换为 EPON 模式或 GPON 模式，且切换的时间间隔应不少于 30 s
配置认证参数	4	**epon-mac-address** *mac-address* 例如：[Huawei-Pon1/0/0] **epon-mac-address 1111-2222-3333**	（三选一）配置设备进行基于物理标识认证时使用的 MAC 地址，格式为 H-H-H，其中 H 为 4 位的十六进制数。但这里配置的认证方式一定要与 OLT 预先分配的认证参数一致，用户无法任意配置，否则认证将无法通过 基于 MAC 认证通过后，禁止用户更改 MAC 地址，以确保设备 MAC 地址唯一

（续表）

<table>
<tr><th>配置任务</th><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td rowspan="3">配置认证参数</td><td rowspan="3">4</td><td>epon-loid loid
例如：[Huawei-Pon1/0/0] epon-loid hwloid</td><td rowspan="2">（三选一）配置基于逻辑标识认证（两种方式可独立，或同时配置）</td><td>（二选一）配置设备进行基于逻辑标识认证时使用的逻辑标识，1～24 个字符，不支持空格，但也与 OLT 预先分配的认证参数一致，用户无法任意配置，否则认证将无法通过
在同一个视图下重复执行 epon-loid 命令后，新配置覆盖老配置</td></tr>
<tr><td>epon-checkcode checkcode
例如：[Huawei-Pon1/0/0] epon-checkcode eponcode</td><td>（二选一）配置设备进行基于逻辑标识认证时使用的校验码 1～12 个字符，不支持空格，但也是与 OLT 预先分配的认证参数一致，用户无法任意配置，否则认证将无法通过
在同一个视图下重复执行 epon-checkcode 命令后，新配置覆盖老配置</td></tr>
<tr><td>epon-password cipher password
例如：[Huawei-Pon1/0/0] epon-password cipher hwpwd</td><td colspan="2">（三选一）配置设备进行密码模式认证时使用的密码为 1～32 个字符，区分大小写，不支持空格，但也与 OLT 预先分配的认证参数一致，用户无法任意配置，否则认证将无法通过
在同一个视图下重复执行 epon-password 命令后，新配置覆盖老配置
密码模式认证方式为华为技术有限公司私有认证方式，对接的 OLT 设备也需为华为技术有限公司设备</td></tr>
<tr><td>（可选）配置光模块参数</td><td>5</td><td>laser { auto | off | on [time-value] }
例如：[Huawei-Pon1/0/0] laser on 30</td><td colspan="2">配置当前 PON 接口光模块的发光模式。命令中的参数和选项说明如下
● auto：多选一选项，指定当前 PON 接口光模块为正常发光模式，当需要光模块正常工作时选择该模式
● off：多选一选项，指定当前 PON 接口光模块为关闭模式，当需要光模块不发光时选择该模式。此时请确认该接口没有承载业务，否则会造成业务中断
● on：多选一选项，指定当前 PON 接口光模块为长发光模式，当需要测试光模块的发光功率时选择该模式
● time-value：可选参数，设置光口长发光时间，取值范围为（1～60）整数秒，缺省值为 20 s。当长发光时间过后，光模块发光模式将会自动切换为正常发光模式
【注意】当前 PON 口模式为 GPON 时，不能直接从 off 模式切换到 on 模式，必须先切换到 auto 模式，再切换为 on 模式
缺省情况下，PON 接口光模块的发光模式为 auto</td></tr>
</table>

（续表）

配置任务	步骤	命令	说明
（可选）配置光模块参数	6	**optical-module threshold bias** { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }* 例如：[Huawei-Pon1/0/0] **optical-module threshold bias lower-limit** 5 **upper-limit** 50	配置光模块偏置电流告警低门限和高门限值。命令中的参数说明如下 ● *lower-limit*：可多选参数，指定偏置电流告警低门限，取值范围为 0～10 000 整数 mA，推荐使用值为 2 mA。如果同时设置上限和下限时，下限不能大于上限 ● *upper-limit*：可多选参数，指定偏置电流告警高门限，取值范围为 0～10 000 整数 mA，推荐使用值为 70 mA 【说明】光模块偏置电流的正常工作范围为 0～10 000 mA，若超出此范围，光模块可能无法正常接收光信号，将导致 ONU 业务中断和下线。可使用此命令设置偏置电流上下限值，当偏置电流超出上下限时，ONU 会向网管设备发送告警 在同一个视图下重复执行 **optical-module threshold bias** 命令后，新配置覆盖老配置
	7	**optical-module threshold rx-power** { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }* 例如：[Huawei-Pon1/0/0] **optical-module threshold rx-power lower-limit** -25 **upper-limit** 50	配置光模块接收光功率告警低门限和高门限值。命令中的参数说明如下 ● *lower-limit*：可多选参数，指定接收光功率告警低门限，为一浮点数类型，小数点后保留 2 位，取值范围为–99.00～100.00 dBm，推荐使用值为–35.00 dBm。如果同时设置上限和下限时，下限不能大于上限 ● *upper-limit*：可多选参数，指定接收光功率告警高门限，为一浮点数类型，小数点后保留 2 位，取值范围为–99.00～100.00 dBm，推荐使用值为 1.00 dBm 【说明】光模块接收光功率的正常工作范围为–99.00～100.00dBm，若超出此范围，光模块可能无法正常接收光信号，将导致 ONU 业务中断和下线。可使用此命令设置接受光功率上下限值，当接受光功率超出上下限时，ONU 会向网管设备发送告警 在同一个视图下重复执行 **optical-module threshold rx-power** 命令后，新配置覆盖老配置
	8	**optical-module threshold tx-power** { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }* 例如：[Huawei-Pon1/0/0] **optical-module threshold tx-power lower-limit** -25 **upper-limit** 50	配置光模块发送光功率告警低门限和高门限值。命令中的参数说明如下 ● *lower-limit*：可多选参数，指定发送光功率告警低门限，为一浮点数类型，小数点后保留 2 位，取值范围为–99.00～100.00 dBm，推荐使用值为–1.00 dBm。如果同时设置上限和下限时，下限不能大于上限 ● *upper-limit*：可多选参数，指定发送光功率告警高门限，为一浮点数类型，小数点后保留 2 位，取值范围为–99.00～100.00 dBm，推荐使用值为 7.00 dBm 【说明】光模块发送光功率的正常工作范围为–99.00～100.00 dBm，若超出此范围，光模块可能无法正常接收光信号，将导致 ONU 业务中断和下线。可使用此命令设置发送光功率上下限值，当发送光功率超出上下限时，ONU 会向网管设备发送告警 在同一个视图下重复执行 **optical-module threshold tx-power** 命令后，新配置覆盖老配置

（续表）

配置任务	步骤	命令	说明
（可选）配置光模块参数	9	**optical-module threshold temperature** { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }* 例如：[Huawei-Pon1/0/0] **optical-module threshold temperature lower-limit -45 upper-limit 45**	配置光模块温度告警低门限和高门限值。命令中的参数说明如下 ● *lower-limit*：可多选参数，指定光模块温度告警低门限，为一浮点数类型，小数点后保留2位，取值范围为-99.00～300.00℃，推荐使用值为-10℃。如果同时设置上限和下限时，下限不能大于上限 ● *upper-limit*：可多选参数，指定光模块温度告警高门限，为一浮点数类型，小数点后保留2位，取值范围为-99.00～100.00℃，推荐使用值为100℃ 【说明】光模块温度的正常工作范围为-99.00～300.00℃，若超出此范围，光模块可能无法正常接收光信号，将导致ONU业务中断和下线。可使用此命令设置光模块温度上下限值，当光模块的温度超出上下限时，ONU会向网管设备发送告警 在同一个视图下重复执行 **optical-module threshold temperature** 命令后，新配置覆盖老配置
	10	**optical-module threshold voltage** { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }* 例如：[Huawei-Pon1/0/0] **optical-module threshold voltage lower-limit 5 upper- limit 25**	配置光模块电压告警低门限和高门限值。命令中的参数说明如下 ● *lower-limit*：可多选参数，指定光模块电压告警低门限，为一浮点数类型，小数点后保留2位，取值范围为0～100.00 V，推荐使用值为2.97 V。如果同时设置上限和下限时，下限不能大于上限 ● *upper-limit*：可多选参数，指定光模块温度告警高门限，为一浮点数类型，小数点后保留2位，取值范围为0～100.00 V，推荐使用值为3.63 V 【说明】光模块电压的正常工作范围为0～100.00 V，若超出此范围，光模块可能无法正常接收光信号，将导致ONU业务中断和下线。可使用此命令设置电压上下限值，当光模块的电压超出上下限时，ONU会向网管设备发送告警 在同一个视图下重复执行 **optical-module threshold voltage** 命令后，新配置覆盖老配置
【说明】当用户需要取消以上步骤6～10所配置的所有光模块告警门限时，可以执行 **undo optical-module threshold** 命令。执行本命令后，设备将取消所有已配置的光模块告警门限，当偏置电流、接收光功率、发送光功率、温度或电压过高或过低时，ONU不会向网管设备发送告警			

3.11.3 配置GPON接口

当需要与GPON网络连接时，则需要配置PON接口为GPON接口。通过配置GPON接口属性可使路由器与上行OLT设备完成对接。在配置GPON接口之前，需在路由器上成功安装、注册PON接口卡。

GPON接口的配置任务与上节介绍的EPON接口卡的配置任务类似，包括以下配置任务。

（1）配置工作模式

为了实现设备与支持GPON模式的OLT的顺利对接，用户可以选择设备工作在自

适应模式下，也可以手动配置设备的PON接口与对接设备的PON接口使其工作在GPON模式下。

配置GPON模式的方法是在PON接口视图下使用**port mode gpon**命令，缺省情况下，PON接口的工作模式为自适应（**adapt**）模式。当PON接口上配有业务时，切换模式会导致业务中断，请谨慎操作。

推荐使用自适应模式，但是在自适应模式下只能自适应成功一次。例如，设备的PON接口已经成功自适应为EPON模式，当再次接入到OLT的PON接口下时，如果OLT的PON接口工作在GPON模式下，只有重启PON单板才能自适应成功。

（2）配置认证参数

OLT也需要对ONU的有效性和合法性进行认证，以防非法ONU接入。GPON系统支持表3-30所示的两种ONU认证方式。

表3-30　GPON系统支持的两种ONU认证方式及比较

ONU认证方式	说明	优点	缺点	应用场景
SN认证	采用ONU的SN作为认证标识的认证方法。ONU的SN是全球唯一的，由13个字符组成。前面4个字符代表生产厂家，华为技术有限公司生产的ONU的前4个字符为"hwhw"	**无需用户手动配置**，可靠性高	当ONU损坏需要更换新ONU时，OLT上需添加新ONU的SN，无法即插即用	因为设备天然支持SN认证，所以适用于所有场景
密码认证	采用ONU上报的密码和OLT预配置密码进行校验的认证方法	配置简单，用户在变换物理位置时，不需要重新配置密码，提高了终端用户接入的灵活性	若非法ONU盗取了合法ONU的密码，OLT进行认证时，最先通过认证ONU的业务先上线，可能会导致合法ONU无法正常上线	适用于移动性需求比较高的场景

在ONU上配置的认证参数由OLT预先分配，用户无法任意配置，否则认证将无法通过。可在PON接口视图下使用**gpon-password cipher** *password*命令配置OLT采用密码模式认证时使用的密码，为1～10个字符，区分大小写，不支持空格。在同一个视图下重复执行本命令后，新配置覆盖老配置。**设备缺省支持SN认证，无需用户配置。**

GPON系统对ONU进行认证有三种处理方式：仅采用SN认证、仅采用密码认证或采用SN和密码组合认证。当GPON系统采用密码认证，或SN和密码组合认证时，执行**gpon-password** *password*命令配置ONU向OLT注册时使用的密码。仅采用SN认证时无需另外配置。

（3）（可选）配置光模块属性

这方面与上节介绍的EPON接口光模块属性配置完全一样，可直接参见上节表3-29中的第5～10步。

3.11.4 PON接口管理

在日常维护中，可使用以下**display**任意视图命令检查配置结果，管理PON接口，

也可用以下 **reset** 用户视图命令清除 PON 接口上的统计信息（当你需要统计一定时间内 PON 接口生成的串口的流量信息时，必须在统计开始前清除该接口下原有的统计信息，重新进行统计）。

① **display epon-info interface pon** *interface-number*：查看 EPON 接口信息，包括 EPON 接口的发光模式、信号是否同步、逻辑链路标识、加密开关状态、加密模式、环回模式、MAC 地址、密码、逻辑标识、校验码等信息。

② **display pon-transceiver interface pon** *interface-number*：查看 PON 接口光模块信息，包括查看到 PON 接口光模块的光波波长、标识、传输距离、版本信息、偏置电流、供电电压等信息。

③ **display pon-statistic interface pon** *interface-number*：查看 PON 接口流量统计信息，包括查看到 PON 接口接收帧、接收字节、上下行以太帧统计数、上下行实时流量等信息。

④ **reset pon-statistic interface pon** *interface-number*：清除指定 EPON 和 GPON 接口的报文统计信息。

3.12 ADSL 接口配置与管理

ADSL（Asymmetric Digital Subscriber Line，不对称数字用户线）是一种非对称的传输技术，利用了普通电话线中未使用的高频段，在双绞铜线上实现高速数据传输。当路由器作为 CPE（Customer Premises Equipment，用户端设备）部署时，为了使 ADSL 线路上业务的正常传输，首先要去激活 ADSL 接口，然后配置 ADSL 接口的上行线路参数，最后激活 ADSL 接口。

3.12.1 ADSL 概述

ADSL 采用频分复用技术把普通电话线分成了普通电话信道、上行信道、下行信道，从而避免了相互之间的串扰，并且提供通道化数据业务 E1/Tl、帧中继、IP 和 ATM 等，实现了高速率的视频、音频等数据信号的传送，并可实现高速数据传输。

1. ADSL 技术演进

G.992.1（G.dmt）、G.992.2（G.lite）是 ITU 发布的第一代 ADSL 标准，支持上行速率 640 kbit/s 到 2 Mbit/s，下行速率 1 Mbit/s 到 8 Mbit/s，其有效的传输距离在 3～5 km。自 1999 年 6 月发布以来，ITU 对 ADSL 的传输性能、抗线路损伤、射频干扰能力、线路诊断和运行维护等方面不断进行了改进。2002 年，ITU 公布了 ADSL 的两个新标准（G.992.3 和 G.992.4），也就是 ADSL2。2003 年，在新一代 ADSL2 标准的基础上，ITU 又制定了 G.992.5，也就是 ADSL2+。

ADSL2/ADSL2+使用的频段与 ADSL 相同，但具有如下特点。

① 传输速率更高：ADSL2 理论上最快的下行速率是 12 Mbit/s，上行速率是 1 Mbit/s；ADSL2+对使用的频谱进行扩展，下行最大传输速率可达 24 Mbit/s，上行速率为 1 Mbit/s。

② 传输距离更远：除了在速率上的提升之外，ADSL2/2+还通过提高调制效率、减小帧开销、提高编码增益、采用更高级的信号处理算法等措施，使长距离、受射频干扰

等情况下的传输性能得到了进一步改善。目前 ADSL 只能在 3 km 左右达到正常速率，用户线最长有 5 km，长距离下速度仅有 3 km 时的 1/4；而 ADSL2+的距离可达 6 km，可以更好地解决一些边远地区的上网问题。

③ 功耗更低：第一代 ADSL 不论是否有数据传输，功率始终相同。ADSL2/2+支持收发器在数据传输速率低或无数据传送时进入休眠状态，可大大降低功耗和散热要求。

2. ADSL 系统结构

ADSL 系统主要由局端设备 DSLAM（Digital Subscriber Line Access Multiplexer，数字用户线路访问复用器）和用户端设备 CPE 组成，如图 3-31 所示。DSLAM 是放置在局端的终结 ADSL 协议的汇聚设备；CPE 是位于客户端的给用户提供各种接口的用户侧终端，用来对用户的数据进行调制和解调，并利用 ADSL 技术，将用户的数据上传至 DSLAM 设备。此处讲的 AR G3 路由器是作为 CPE 来部署的。

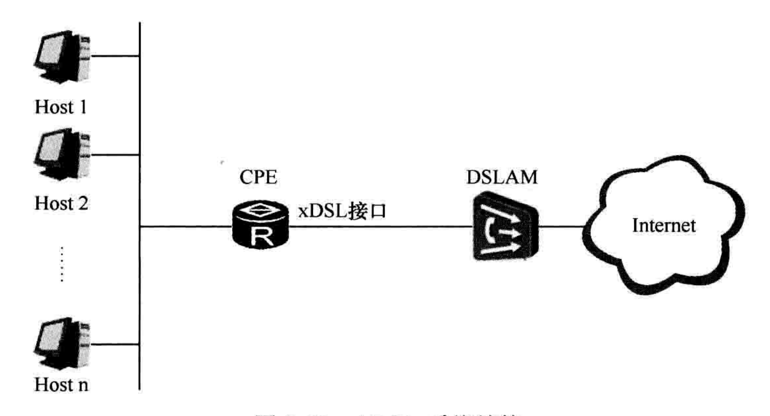


图 3-31 ADSL 系统结构

在 ADSL 系统中，DSLAM 到 CPE 的数据传输方向称之为下行方向，反之为上行方向。因此路由器的 ADSL 接口亦称之为 ADSL 上行接口。

3.12.2 ADSL 主要特性

在 AR G3 系列路由器中，仅 AR156、AR157、AR206 和 AR207/207-S 直接支持 ADSL 接口；AR1200/1200-S 系列、AR2204/2204-S、AR2220L、AR2220/2200-S、AR2240/2240-S 和 AR3200 系列可通过 ADSL 单板（ADSL-A/M 或 ADSL-B 接口卡）支持 ADSL 接口。

1. ADSL 线路激活

线路激活是指局端设备与 CPE 设备之间进行协商，协商内容包括传输标准、上下行线路速率、规定的噪声容限等，并检测线路距离和线路状况，确认 CPE 设备能否在上述条件下正常工作。如果协商成功，则局端与 CPE 设备建立通信连接，称为接口激活。接口激活后，就可以在局端与 CPE 设备之间传输业务了。

设备启动后，ADSL 接口自动进入激活状态。只要线路良好，接口就应该始终处于激活状态。但当 ADSL 接口上需要配置上行线路参数以实现 CPE 和局端设备的对接时，需先将 ADSL 接口去激活，然后配置 ADSL 上行线路参数，最后重新激活，使配置生效。

2. ADSL 接口的上行线路参数

ADSL 接口的上行线路参数包括传输标准、比特交换开关、无缝自适应速率开关和

格栅编码开关。下面分别予以介绍。

（1）ADSL 传输标准

为保证业务流在 ADSL 线路上正常传输，需要配置 ADSL 接口的传输标准。AR G3 系列路由器 ADSL 接口支持表 3-31 所示的传输标准。当路由器作为 CPE 部署时，选择的传输标准需与局端保持一致。推荐将传输标准配置为自适应方式，设备将根据局端的传输标准，从 G.DMT、ADSL2、AnnexL、ADSL2+、AnnexM、AnnexJ 和 T1.413 中自动选择与局端相同的标准激活。

表 3-31　　AR G3 系列路由器 ADSL 接口支持的传输标准

ADSL 传输标准	说明
G.DMT(G992.1)	其频谱为上行 25～138 kHz，下行 138～1 104 kHz，上行速率可达到 1 Mbit/s，下行速率可达到 8 Mbit/s
ADSL2(G992.3)	ADSL2 通过改善调制速率、提高编码增益、减少帧头开销、改善初始化状态机、使用增强的信号处理算法，在和 ADSL 同样的频段上速率有了进一步的提高，上行速率可达到 1 Mbit/s，下行速率可达到 12 Mbit/s
AnnexL	ADSL2 附件中规定了 Reach extended ADSL2 标准，简称为 AnnexL，通过使用更窄的频带和对发送功率谱模板的优化，使得其在远距离的传输中获得较好的性能 【说明】AR1200 系列、AR2204、AR2220L、AR2220、AR2240 和 AR3200 系列支持的 ADSL 单板分为 ADSL-A/M 和 ADSL-B/J，**仅 ADSL-A/M 支持此标准**。AR150/200 系列只有 AR157、AR157W、AR157VW、AR157G-HSPA+7、AR207、AR207V、AR207VW、AR207V-P、AR207G-HSPA+7 支持此标准
ADSL2+(G992.5)	使用频带范围扩展到 2.208 MHz，上行速率可达到 1 Mbit/s，下行速率可达到 24 Mbit/s
AnnexM	AnnexM 通过对 ADSL2 或 ADSL2+标准上行频带的扩展，上行速率可达到 2 Mbit/s 【说明】AR1200/1200-S 系列、AR2204/2204-S、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3200 系列支持的 ADSL 单板分为 ADSL-A/M 和 ADSL-B，**仅 ADSL-A/M 支持此标准**。AR150/150-S/200/200-S 系列只有 AR157、AR157W、AR157VW、AR157G-HSPA+7、AR207/207-S、AR207V、AR207VW、AR207V-P、AR207G-HSPA+7 支持此标准
AnnexJ	表示支持对 ADSL2 或 ADSL2+标准上行频带扩展，上行速率可达到 3 078 kbit/s 【说明】AR1200/1200-S 系列、AR2204/2204-S、AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3200 系列支持的 ADSL 单板分为 ADSL-A/M 和 ADSL-B，**仅 ADSL-B/J 单板支持此标准**。AR150/200 系列中，只有 AR156 和 AR206 的 ADSL 接口支持此标准
T1.413	全速率 ADSL，上行速率可达到 1 Mbit/s，下行速率可达到 8 Mbit/s 【说明】AR1200 系列、AR2204、AR2220L、AR2220、AR2240 和 AR3200 系列支持的 ADSL 单板分为 ADSL-A/M 和 ADSL-B/J，**仅 ADSL-A/M 支持此标准**。AR150/200 系列只有 AR157、AR157W、AR157VW、AR157G-HSPA+7、AR207、AR207V、AR207VW、AR207V-P、AR207G-HSPA+7 支持此标准

（2）比特交换

在线路激活过程中，每个子信道独立计算信噪比和承载比特，但在线路激活后，线路的信噪比可能会因外界环境因素发生变化，有的子信道的信噪比因此而变小，有的因此而变大，这种变化若长时间维持可能会导致线路掉线。比特交换的目的就是让这些信噪比较低的子信道转移一些它们的比特到信噪比较高的子信道上去，或者减小信噪比较

高子信道上的发送功率，然后把多出来的发送功率加到信噪比较低的子信道上，通过增加它们的发送功率来提高信噪比，从而降低误码率，同时这个动态调整过程中线路不会重新协商。

（3）无缝速率自适应

当外界环境因素发生变化时，为避免线路掉线，在不用激活线路的情况下，可打开比特交换开关，实现在子信道的内部之间进行比特分布的调整或功率调整。但比特交换的能力是有限的，而且它并不能改变线路速率，当线路环境变得很恶劣时，通过比特交换已不能满足线路误码要求，此时可依靠 SRA（Seamless Rate Adaptation，无缝速率自适应）技术来解决。它能动态无缝地调节线路的速率，而无需重新激活线路。

（4）格栅编码

格栅编码是指通过特殊的编码算法达到较好的编码效益，以提高线路的信噪比增益。在线路格栅编码开关打开之后，激活速率会比不打开的情况下有较大幅度的提高。

3.12.3 配置 ADSL 接口

配置了 ADSL 接口后，设备可以将业务上传至上层设备。但在配置 ADSL 接口之前，如果是 AR1200/1200-S 系列、AR2204、AR2220L、AR2220/2200-S、AR2240 和 AR3200 系列，则需要在路由器上将 ADSL-A/M 或 ADSL-B 接口卡注册成功。

ADSL 接口的主要配置任务包括以下三个方面。

（1）去激活 ADSL 接口

缺省情况下，ADSL 接口处于激活状态。设备启动后，ADSL 接口自动进入激活状态。当 ADSL 接口上需要配置上行线路参数，以实现 CPE 和局端设备的对接时，**必须先将 ADSL 接口去激活**，然后配置 ADSL 参数，最后重新激活，使配置生效。

（2）配置 ADSL 接口的上行线路参数

当设备的 ADSL 接口已去激活后，可以为 ADSL 接口配置传输标准、比特交换功能、无缝自适应速率功能和格栅编码功能，**但均需要与局端保持一致，否则不能与局端设备建立通信。但各参数配置任务没有严格的先后次序。**

（3）激活 ADSL 接口

已配置了 ADSL 接口的上行线路参数后，需要再次重新激活 ADSL 接口，以使设备与局端建立通信连接，进行业务传输。

以上 ADSL 接口配置任务的具体配置步骤如表 3-32 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表 3-32 ADSL 接口配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**interface atm** *interface-number* 例如：[Huawei] **interface atm 1/0/0**	进入 ADSL 接口视图

（续表）

配置任务	步骤	命令	说明
去激活 ADSL 接口	3	**shutdown** 例如：[Huawei-Atm1/0/0] **undo shutdown**	去激活 ADSL 接口
配置 ADSL 接口的上行线路参数	4	**adsl standard** { **adsl2** [**annexm**] | **adsl2+** [**annexm**] | **annexl** | **auto** | **gdmt** | **t1413** } 例如：[Huawei-Atm1/0/0] **adsl standard t1413**	配置 ADSL 接口的传输标准。命令中的选项说明如下 ● **adsl2**：多选一选项，指定 ADSL 接口的传输标准为 ADSL2(G992.3)标准 ● **adsl2+**：多选一选项，指定 ADSL 接口的传输标准为 ADSL2+(G992.5)标准 ● **annexl**：多选一选项，指定 ADSL 接口的传输标准为 AnnexL 标准 ● **auto**：多选一选项，指定 ADSL 接口的传输标准为自适应方式。选择自适应方式，当前设备将根据对端设备的传输标准，从 G.DMT、ADSL2、AnnexL、ADSL2+、AnnexM、T1.413 中自动选择与对端相同的标准激活 ● **gdmt**：多选一选项，指定 ADSL 接口的传输标准为 G.DMT(G992.1)标准 ● **t1413**：多选一选项，指定 ADSL 接口的传输标准为 T1.413 标准 ● **annexm**：可选项，表示支持对 ADSL2 或 ADSL2+ 标准上行频带扩展，上行速率可达到 2 Mbit/s，但仅 ADSL-A/M 单板支持此可选项 缺省情况下，ADSL 接口的传输标准为 **auto** 设备默认开启 AnnexM 标准，若需以 AnnexM 标准激活，需要保证在局端设备同时开启 AnnexM 标准
	5	**adsl bitswap** { **off** | **on** } 例如：[Huawei-Atm1/0/0] **adsl bitswap off**	配置打开（选择 **on** 选项时）或关闭（选择 **off** 选项时）ADSL 接口的比特交换开关。对接的两端设备必须都打开了比特交换开关，线路重新激活后比特交换功能才生效 缺省情况下，ADSL 接口的比特交换开关处于打开状态
	6	**adsl sra** { **off** | **on** } 例如：[Huawei-Atm1/0/0] **adsl sra off**	配置打开（选择 **on** 选项时）或关闭（选择 **off** 选项时）ADSL 接口的无缝速率自适应开关。对接的两端设备必须都打开了无缝速率自适应开关，线路激活后无缝速率自适应功能才生效 缺省情况下，ADSL 接口的无缝速率自适应开关处于关闭状态
	7	**adsl trellis** { **off** | **on** } 例如：[Huawei-Atm1/0/0] **adsl trellis off**	配置打开（选择 **on** 选项时）或关闭（选择 **off** 选项时）ADSL 接口的格栅编码开关。对接的两端设备必须都打开了格栅编码开关，线路激活后格栅编码功能才生效 缺省情况下，ADSL 接口的格栅编码开关处于打开状态
激活 ADSL 接口	8	**undo shutdown** 例如：[Huawei-Atm1/0/0] **undo shutdown**	激活 ADSL 接口 ADSL 接口去激活后，设备与局端建立通信的连接不再存在，如果要进行业务传输，则必须重新激活该接口，以使以上 ADSL 接口的上行线路参数配置生效

3.12.4 ADSL 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 ADSL 接口。

① **display dsl interface atm** *interface-number*：查看 ADSL 接口的状态信息，包括查看 ADSL 接口是否与局端 ADSL 接口协商成功、接口所配置的传输标准、线路状态信息、性能统计信息、比特交换开关是否打开、无缝速率自适应开关是否打开、格栅编码开关是否打开以及单板版本信息。

② **display interface atm** [*interface-number*]：查看 ADSL 接口的配置和性能统计信息，用户可以根据这些信息进行流量统计和接口的故障诊断等。

3.12.5 ADSL 接口上行配置示例

本示例网络结构如图 3-32 所示，企业 A 中多个主机统一接入企业网关（AR G3 系列路由器），上行通过 ADSL 线路接入 DSLAM。运营商向企业 A 提供一条 ADSL 线路满足企业用户的业务需求。这时设备的上行接口需为 ADSL 接口，设备通过 ADSL 接口实现与 DSLAM 设备的对接。

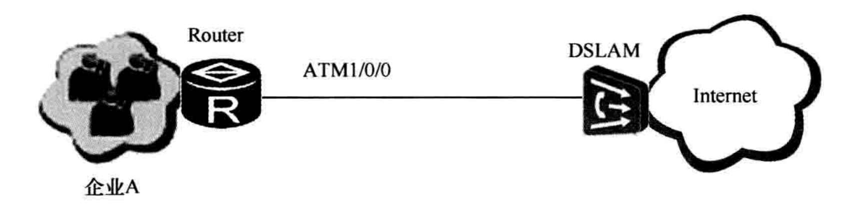


图 3-32 ADSL 接口上行配置示例基本网络结构

本示例的配置很简单，可直接根据 3.12.3 小节介绍的配置步骤进行配置。根据局端的线路参数，在设备上配置相同的线路参数，使设备对接成功。局端设备 ADSL 线路参数：传输标准为 ADSL2+，比特交换开关和格栅编码开关均处于打开状态，无缝速率自适应开关处于关闭状态。但在配置 ADSL 上行参数前，需去激活接口，参数配置完成后，再激活 ADSL 接口，使设备与局端建立连接。

具体的配置步骤如下。

① 去激活接口 ATM1/0/0。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface atm 1/0/0
[Router-Atm1/0/0] shutdown
```

② 根据局端设备参数配置，配置 ADSL 上行线路参数。

```
[Router-Atm1/0/0] adsl standard adsl2+    !—配置设备的 ADSL 接口传输标准为 ADSL2+
[Router-Atm1/0/0] adsl bitswap on         !—打开设备的 ADSL 接口比特交换开关
[Router-Atm1/0/0] adsl sra off            !—关闭设备的 ADSL 接口无缝速率自适应开关
[Router-Atm1/0/0] adsl trellis on         !—打开设备的 ADSL 接口格栅编码开关
```

③ 激活接口 ATM1/0/0。

```
[Router-Atm1/0/0] undo shutdown
[Router-Atm1/0/0] quit
```

最后可通过 **display dsl interface atm** 1/0/0 命令查看设备的 ADSL 接口是否协商成

功、配置的传输标准、线路状态信息、性能统计信息、比特交换开关是否打开、无缝速率自适应开关是否打开、格栅编码开关是否打开以及单板版本信息，验证配置结果。还可通过 **display interface atm** 1/0/0 命令查看设备的 ADSL 接口的配置和状态信息。具体输出示例略。

3.13 VDSL 接口配置与管理

VDSL（Very high data rate Digital Subscriber Line，甚高速数字用户环路）是在 DSL 的基础上集成各种接口协议，通过复用上传和下传管道以获取更高的传输速率。通过价格低廉的双绞线，将 LAN 端接入的业务使用 VDSL 线路上传至上层设备。

3.13.1 VDSL 概述

ADSL 技术在提供图像业务方面带宽十分有限，而且成本偏高，这些缺点成了 ADSL 迅速发展的障碍。VDSL 技术作为 ADSL 技术的发展方向之一，是一种先进的数字用户线技术，采用该技术可以进一步满足客户对图像等宽带业务的需求。

VDSL 与 ADSL 相比，主要优势体现在传输速率方面：ADSL 上行数据速率为 640 kbit/s～2 Mbit/s，下行速率为 1 kbit/s～8 Mbit/s；而 VDSL 非对称的上行速率为 0.8Mbit/s～6.4 Mbit/s，下行速率为 6.5 Mbit/s～52 Mbit/s。另外，ADSL 仅支持非对称传输，VDSL 既支持非对称传输，也支持对称传输，具有良好的传输质量，可以实现高清晰度视频会议、视频点播以及电视广播。

与 ADSL 系统一样，VDSL 系统也主要由局端设备 DSLAM 和用户端设备 CPE 组成，如图 3-33 所示。DSLAM 是放置在局端的终结 VDSL 协议的汇聚设备；CPE 是位于客户端的给用户提供各种接口的用户侧终端，实现对用户的数据进行调制和解调，并利用 VDSL 技术，将用户的数据上传至 DSLAM 设备。AR G3 系列路由器作为 CPE 来部署。

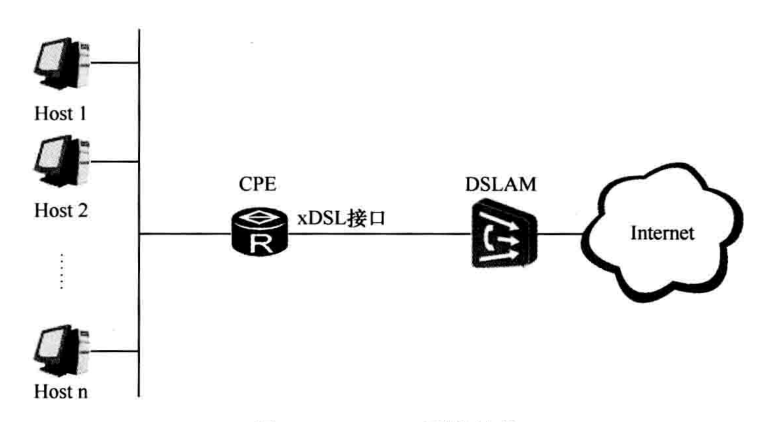


图 3-33 VDSL 系统结构

在 VDSL 系统中，DSLAM 到 CPE 的数据传输方向称之为下行方向，反之为上行方向。因此设备的 VDSL 接口亦称之为 VDSL 上行接口。

3.13.2 VDSL 主要特性

路由器设备在作为 CPE 部署时，为了保证 VDSL 线路上业务的正常传输，首先需要选择 VDSL 接口的工作模式，然后在不同的工作模式下进行配置。在 AR G3 系列路由器中，**仅 AR1200/1200-S 系列、AR2204、AR2220L、AR2220/2200-S、AR2240/2240-S 和 AR3260 支持配置 VDSL 接口。**

1. VDSL 工作模式

设备的 VDSL 接口支持两种工作模式。

① ATM 模式：VDSL 线路承载的是 ATM 信元（分组长度固定为 53 个字节），这就是 PPPoA VDSL 专线模式。

② PTM 模式：VDSL 线路承载的是以太报文，这就是 PPPoE VDSL 拨号模式。因为不需要将以太网帧切片成 ATM 信元再进行传递，省掉了 ATM 传输方式中的 1 483 B/1 483 R 协议封装、AAL5 帧和 ATM 信元的开销，所以 PTM 模式传输以太网业务的效率明显高于 ATM 模式。

在将路由器作为 CPE 部署时，选择何种工作模式是由局端决定的。例如，当局端的 VDSL 接口配置成 ATM 模式时，设备的 VDSL 接口也需配置为 ATM 模式。

2. VDSL 线路激活

线路激活是指局端设备与 CPE 设备之间进行协商，协商内容包括传输标准、上下行线路速率、规定的噪声容限等，并检测线路距离和线路状况，确认能否在上述条件下正常工作。如果协商成功，则局端与 CPE 设备建立通信连接，称为接口激活。接口激活后，就可以在局端与 CPE 设备之间传输业务了。

设备启动后，VDSL 接口自动进入激活状态。当 VDSL 接口上需要配置上行线路参数，以实现 CPE 和局端设备的对接时，与 ADSL 接口一样，也需要先将 VDSL 接口去激活，然后配置 VDSL 参数，最后重新激活 VDSL 接口，使配置生效。

3. VDSL 参数

ATM 模式下 VDSL 接口的参数包括传输标准、比特交换开关、无缝自适应速率开关和格栅编码开关。其中的比特交换开关、无缝自适应速率开关和格栅编码开关技术与 3.12.2 小节介绍的 ADSL 对应技术一样，参见即可。

为保证业务流在 VDSL 线路上正常传输，需要配置 VDSL 接口的传输标准。AR G3 系列路由器 VDSL 接口支持的传输标准如表 3-33 所示。当设备作为 CPE 部署时，选择的传输标准需与局端保持一致。推荐将传输标准配置为自适应方式，设备将根据局端的传输标准，从 G.DMT、ADSL2、AnnexL、ADSL2+、AnnexM、T1.413 和 VDSL2 中自动选择与局端相同的标准激活。

表 3-33 AR G3 系列路由器 VDSL 接口支持的传输标准

VDSL 传输标准	说明
G.DMT(G992.1)	其频谱为上行 25～138 kHz，下行 138～1 104 kHz，上行速率可达到 1 Mbit/s，下行速率可达到 8 Mbit/s
ADSL2(G992.3)	ADSL2 通过改善调制速率、提高编码增益、减少帧头开销、改善初始化状态机、使用增强的信号处理算法，在和 VDSL 同样的频段上速率有了进一步的提高，上行速率可达到 1 Mbit/s，下行速率可达到 12 Mbit/s

（续表）

VDSL 传输标准	说明
AnnexL	ADSL2 附件中规定了 Reach extended ADSL2 标准，简称为 AnnexL，通过使用更窄的频带和对发送功率谱模板的优化，使得其在远距离的传输中获得较好的性能
ADSL2+(G992.5)	使用频带范围扩展到 2.208 MHz，上行速率可达到 1 Mbit/s，下行速率可达到 24 Mbit/s
AnnexM	AnnexM 通过对 ADSL2 或 ADSL2+标准上行频带的扩展，上行速率可达到 2 Mbit/s
T1.413	全速率 ADSL，上行速率可达到 800 kbit/s，下行速率可达到 8 Mbit/s
VDSL2	其上行速率可达到 100 Mbit/s，下行速率可达到 100 Mbit/s。设备不支持手动配置 VDSL2 传输标准，VDSL2 传输标准是根据局端设备协商激活的

3.13.3　配置 ATM 模式下 VDSL 接口

ATM 模式下的 VDSL 接口承载的是 ATM 信元。为使 VDSL 线路获得最佳使用效果，需在路由器上配置 ATM 模式下的 VDSL 接口上相关参数。但在配置 VDSL 接口上行参数之前，需要确保 VDSL 接口卡在路由器上成功注册。

VDSL 接口的配置任务与上节介绍的 ADSL 接口配置任务类似，主要包括以下 4 项。

（1）配置 VDSL 接口工作在 ATM 模式

AR G3 系列路由器的 VDSL 接口支持 ATM 和 PTM 这两种工作模式。在 ATM 模式下，VDSL 线路承载的是 ATM 信元；在 PTM 模式下，VDSL 线路承载的是以太报文。

当设备作为 CPE 部署时，选择何种工作模式是由局端决定的。例如，当局端的 VDSL 接口配置成 ATM 模式时，设备的 VDSL 接口也需配置为 ATM 模式。且只有当设备的 VDSL 接口工作模式与局端相同时，设备和局端才能对接。

（2）去激活 VDSL 接口

缺省情况下，VDSL 接口处于激活状态。设备启动后，VDSL 接口自动进入激活状态。但当 VDSL 接口上需要配置上行线路参数，以实现 CPE 和局端设备的对接时，需先将 VDSL 接口去激活，然后配置 VDSL 参数，最后重新激活，使配置生效。

（3）配置上行线路参数

在 VDSL 接口已去激活状态下，可以配置 VDSL 接口的上行线路参数，包括传输标准、比特交换功能、无缝自适应速率功能和格栅编码功能，均需与局端保持一致才能与局端设备建立通信。

（4）激活 VDSL 接口

配置好上行线路参数后，再需要重新激活 VDSL 接口，使配置生效。

以上配置任务的具体配置步骤如表 3-34 所示（**注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序**）。

表 3-34 ATM 模式下的 VDSL 接口配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
配置工作模式	2	**set workmode slot** *slot-id* **vdsl atm** 例如：**set workmode slot 1 vdsl atm**	配置 VDSL 接口工作在 ATM 模式。参数 *slot-id* 用来指定 VDSL 接口所在的槽位号。执行该步骤后，需要重启单板并等待一段时间才能使配置生效 缺省情况下，VDSL 接口工作在 PTM 模式下
去激活 VDSL 接口	3	**interface atm** *interface-number* 例如：[Huawei] **interface atm 1/0/0**	进入 ATM 工作模式下的 VDSL 接口视图，参数 *interface-number* 用来指定 ATM 工作模式下的 VDSL 接口编号
	4	**shutdown** 例如：[Huawei-Atm1/0/0] **undo shutdown**	去激活 VDSL 接口
配置 VDSL 接口的上行线路参数	5	**adsl standard** { **adsl2** [**annexm**] | **adsl2+** [**annexm**] | **annexl** | **auto** | **gdmt** | **t1413** } 例如：[Huawei-Atm1/0/0] **adsl standard t1413**	配置 VDSL 接口的传输标准。其他说明参见 3.12.3 小节表 3-32 中的第 4 步
	6	**adsl bitswap** { **off** | **on** } 例如：[Huawei-Atm1/0/0] **adsl bitswap off**	配置打开（选择 **on** 选项时）或关闭（选择 **off** 选项时）VDSL 接口的比特交换开关。对接的两端设备必须都打开了比特交换开关，线路重新激活后比特交换功能才生效 缺省情况下，VDSL 接口的比特交换开关处于打开状态
	7	**adsl sra** { **off** | **on** } 例如：[Huawei-Atm1/0/0] **adsl sra off**	配置打开（选择 **on** 选项时）或关闭（选择 **off** 选项时）VDSL 接口的无缝速率自适应开关。对接的两端设备必须都打开了无缝速率自适应开关，线路激活后无缝速率自适应功能才生效 缺省情况下，VDSL 接口的无缝速率自适应开关处于关闭状态
	8	**adsl trellis** { **off** | **on** } 例如：[Huawei-Atm1/0/0] **adsl trellis off**	配置打开（选择 **on** 选项时）或关闭（选择 **off** 选项时）VDSL 接口的格栅编码开关。对接的两端设备必须都打开了格栅编码开关，线路激活后格栅编码功能才生效 缺省情况下，VDSL 接口的格栅编码开关处于打开状态
激活 VDSL 接口	9	**undo shutdown** 例如：[Huawei-Atm1/0/0] **undo shutdown**	激活 VDSL 接口 VDSL 接口去激活后，设备与局端建立通信的连接不再存在，如果要进行业务传输，则必须重新激活该接口，以使以上 VDSL 接口的上行线路参数配置生效

3.13.4 配置 PTM 模式下 VDSL 接口

当需要 VDSL 线路承载以太报文时，可配置 VDSL 接口工作在 PTM 模式。同样，在配置 VDSL 接口之前，需要在路由器上成功安装、注册 VDSL 接口卡。

只有设备的 VDSL 接口工作模式与局端相同时，设备和局端才能对接。例如，当局端的 VDSL 接口配置成 PTM 模式时，设备的 VDSL 接口也需配置为 PTM 模式。因为不

需要将以太网帧切片成 ATM 信元再进行传递，省掉了 1 483 B/1 483 R 封装、AAL5 帧、ATM 信元的开销，所以 PTM 模式传输以太网业务的效率明显高于 ATM 模式。

PTM 模式下的 VDSL 接口配置很简单，主要有以下两个方面。

① 在系统视图下通过 **set workmode slot** *slot-id* **vdsl** { **atm** | **ptm** }命令配置 VDSL 接口工作在 PTM 模式。但缺省情况下，VDSL 接口已工作在 PTM 模式下，所以新设备一般不用配置。执行该步骤后，需要重启单板并等待一段时间才能使配置生效。

② 在 VDSL 接口视图下通过 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]命令为 VDSL 接口配置 IP 地址。参数 *ip-address* 用来为 VDSL 接口配置主 IP 地址，*mask* | *mask-length* 分别用来为配置的 IP 地址指定子网掩码和子网掩码长度；可选项 **sub** 用来指定所配置的 IP 地址为从 IP 地址，如果不选此可选项，则表明所配置的 IP 地址是主 IP 地址。

3.13.5　VDSL 接口管理

在日常维护中，可使用以下 **display** 任意视图命令检查配置结果，管理 VDSL 接口。

① **display dsl interface atm** *interface-number*：查看 ATM 模式下 VDSL 接口的状态信息，包括查看 VDSL 接口是否与局端 VDSL 接口协商成功、接口所配置的传输标准、线路状态信息、性能统计信息、比特交换开关是否打开、无缝速率自适应开关是否打开以及格栅编码开关是否打开。

② **display interface atm** *interface-number*：查看 ATM 模式下 VDSL 接口的配置和性能统计信息，用户可以根据这些信息进行流量统计和接口的故障诊断等。

③ **display interface ethernet** *interface-number*：查看 PTM 工作模式下的 VDSL 接口的配置和状态信息，用户可以根据这些信息进行流量统计和接口的故障诊断等。

3.13.6　VDSL 接口上行配置示例

本示例拓扑结构参见 3.12.5 小节中的图 3-32。企业 A 中多个主机统一接入企业网关设备（AR G3 系列路由器），设备上行通过 VDSL 线路接入 DSLAM。运营商可向企业 A 提供一条 VDSL 线路满足企业用户的业务需求。这时设备的上行接口需要为 VDSL 接口，设备通过 VDSL 接口实现与 DSLAM 设备的对接。

现已知局端设备 VDSL 线路参数为：传输标准为自适应模式，比特交换开关和格栅编码开关均处于打开状态，无缝速率自适应开关处于关闭状态。

本示例的配置同样非常简单，先配置好 VDSL 接口工作模式（此处仅以 ATM 模式进行介绍），并去激活 VDSL 接口，然后根据已知的局端的线路参数，在设备上配置相同的线路参数，配置好后再激活 VDSL 接口，使设备对接成功。

具体的配置步骤如下。

① 配置设备的 VDSL 接口工作在 ATM 模式下。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] set workmode slot 1 vdsl atm
Changing the working mode will reset the board in slot 1. Continue? [y/n]:y
INFO: Resetting board[1] succeeded.
```

② 去激活接口 ATM1/0/0 VDSL 接口。

```
[Router] interface atm 1/0/0
[Router-Atm1/0/0] shutdown
```

③ 根据局端设备参数配置，配置 VDSL 上行线路参数。

```
[Router-Atm1/0/0] adsl standard auto    !---配置设备的 VDSL 接口传输标准为自适应方式
[Router-Atm1/0/0] adsl bitswap on       !---打开设备的 VDSL 接口比特交换开关
[Router-Atm1/0/0] adsl sra off          !---关闭设备的 VDSL 接口无缝速率自适应开关
[Router-Atm1/0/0] adsl trellis on       !---打开设备的 VDSL 接口格栅编码开关
```

④ 激活接口 ATM1/0/0。

```
[Router-Atm1/0/0] undo shutdown
[Router-Atm1/0/0] quit
```

最后可使用 **display dsl interface atm** 1/0/0 命令查看设备的 VDSL 接口是否协商成功、配置的传输标准、线路状态信息、性能统计信息、比特交换开关是否打开、无缝速率自适应开关是否打开、格栅编码开关是否打开以及单板版本信息，验证配置结果。还可使用 **display interface atm** 1/0/0 命令查看设备的 VDSL 接口的状态和统计信息。具体输出示例略。

3.14 G.SHDSL 接口配置与管理

G.SHDSL（G.Single-pair High Speed Digital Subscriber Line，单对高速数字用户线）是一种高速对称的传输技术，利用了普通电话线中未使用的高频段，在双绞铜线上实现高速数据传输。

3.14.1 G.SHDSL 概述

在 AR G3 系列路由器，**仅 AR158E、AR158EVW、AR208E 系列直接**提供 G.SHDSL 接口，AR1200/1200-S、AR2204/2204-S、AR2220L、AR2220/2220-S、AR2240 和 AR3200 系列可通过使用的 4G.SHDSL 单板虚拟出 4 个 G.SHDSL 接口。

由于 ADSL 速率的不对称性，使得 ADSL 的应用存在不少局限，特别是商用宽带需求环境是一个双向的、对称的流量环境，对性能波动的容忍度比较低，ADSL 接入技术已越来越不能满足人们对带宽和流量的需求。于是，G.SHDSL 技术应运而生。

G.SHDSL 是由 ITU-T 定义的在普通双绞线上提供双向对称带宽数据业务传输的一种技术，符合国际电联 G.991.2 推荐标准，由于采用性能优越的 16 电平网格编码脉冲幅度调制技术，压缩了传输频谱，提高了抗噪性能，最大传输距离达 6 km，因此与 ADSL 技术相比有着明显的技术优势。

相对于 ADSL 来说，G.SHDSL 的优势体现在其对称的高速传输速率上，每对双绞线可提供从 192 kbit/s～5.696 Mbit/s 的对称速率，并可通过接口绑定提供更大的带宽，这大大提升了服务范围，改善了服务质量。另外，由于 G.SHDSL 调制方式的优点，同样的速率可得到更长的传输距离；同样的传输距离可获得更高的传输速率；同样的速率和传输距离可提高信噪比容限。这样就使得 G.SHDSL 既能为中小型企业以及大型企业的分支机构提供各种全面的解决方案，满足各种业务需求，如安全、VPN 和业务延展规划，也

可为服务供应商提供解决语音、视频会议等各种集成通信问题的方案。

G.SHDSL 系统结构如图 3-34 所示，主要由局端设备 CO（Central Office）和用户端设备 CPE 组成。CO 是放置在局端的终结 G.SHDSL 协议的汇聚设备；CPE 是位于客户端的给用户提供各种接口的用户侧终端，可对用户的数据进行调制和解调，并利用 G.SHDSL 技术，将用户的数据上传至局端设备。AR G3 系列路由器既可以作为 CPE 来部署，也可以作为 CO 来部署。在 G.SHDSL 系统中，CO 到 CPE 的数据传输方向称之为下行方向，反之为上行方向。因此 CPE 设备的 G.SHDSL 接口亦称之为 G.SHDSL 上行接口。

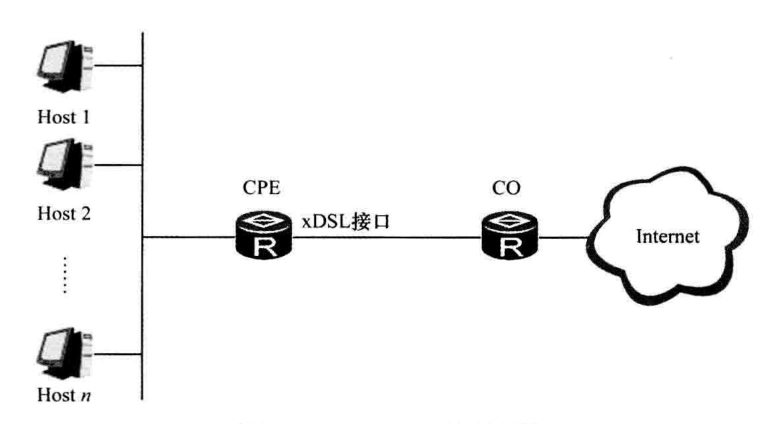


图 3-34 G.SHDSL 系统结构

G.SHDSL 接口的传输模式也分 ATM 和 PTM 两种（**要与局端设备的传输模式一致**），下面分别介绍这两种传输模式下的 G.SHDSL 接口配置方法。

3.14.2 G.SHDSL 接口配置任务

与前面介绍的 ADSL 接口和 VDSL 接口配置任务相比，G.SHDSL 接口可以配置的参数更多，更复杂些，主要包括如下配置任务（**下面的第 3 项到第 11 项配置任务中的各参数配置任务没有严格的先后次序**）。

（1）配置 G.SHDSL 接口的传输模式

G.SHDSL 接口支持两种传输模式：ATM 模式和 PTM 模式。ATM 模式下，G.SHDSL 线路承载的是 ATM 信元；PTM 模式下，G.SHDSL 线路承载的是以太报文。当设备作为 CPE 部署时，选择何种传输模式是由局端决定的。

（2）去激活 G.SHDSL 接口

设备启动后，G.SHDSL 接口自动进入激活状态。当 G.SHDSL 接口上需要配置上行线路参数，以实现 CPE 和局端设备的对接时，需先将 G.SHDSL 接口去激活，然后配置 G.SHDSL 参数，最后重新激活，使配置生效。

（3）配置 G.SHDSL 接口的工作模式

设备的 G.SHDSL 接口支持两种工作模式：CO（局端）模式和 CPE（客户端）模式。当两台设备在背对背连接时，必须把一端配置为 CO（局端）模式，另一端配置成 CPE（客户端）模式。

（4）配置 G.SHDSL 接口的绑定

为了增加带宽，当局端设备配置了接口绑定时，路由器上需配置与其相同的接口绑定。例如，局端配置了 0 号和 1 号接口绑定，路由器上也必须配置为 0 号和 1 号接口绑定。配置绑定时需注意以下情况。

① 绑定的接口必须是同一单板（4G.SHDSL 接口卡或 SRU 主控板）上的连续几个接口，绑定的接口号必须从偶数开始，开始绑定的接口为主接口，被绑定的接口为从接口。

② 只有待绑定接口均处在去激活状态，且均没有配置业务时，才可配置接口绑定。

（5）配置 G.SHDSL 接口使用的标准

当局端设备配置了传输标准，路由器上需配置与其相同的传输标准。AR G3 系列路由器支持的 G.SHDSL 接口的传输标准如下。

① G.991.2 Annex A 和 G.991.2 Annex F 标准为北美标准。

② G.991.2 Annex B 和 G.991.2 Annex G 标准为欧洲标准。

（6）配置 G.SHDSL 接口的功率频谱密度模式

当局端设备配置了功率频谱密度模式，路由器上需配置与其相同的功率频谱密度模式。AR G3 系列路由器支持的 G.SHDSL 接口的功率频谱密度模式如下。

① 对称模式：对称 PSD 与其他的业务具有良好的频谱兼容性，消耗的功率也更低，适用于短距离传输。

② 非对称模式：非对称 PSD 采用较高的发送功率来实现更佳的传输性能，适用于长距离传输。

（7）配置 G.SHDSL 接口的发射功率

正常情况下，接口会根据线路噪声情况，自动调整发送功率，以保证可以获得合适的信噪比。在线路噪声已知的情况下，或者自动调整不准确的时候，可以通过此命令手动调整发射功率。

（8）配置 G.SHDSL 接口的单板能力

G.SHDSL 接口的单板能力仅支持工作在 ATM 传输模式下的 G.SHDSL 接口。根据局端设备芯片类型不同，用户选择不同的单板能力，要求与局端设备保持一致，以便实现与局端设备的对接。例如，当局端设备为 g-shdsl 模式（还有 g-shdsl.bis 模式）时，设备上也需配置为 g-shdsl 模式，实现对局端设备的对接。

（9）配置 G.SHDSL 上行接口的兼容性模式

接口的兼容性模式仅支持工作在 ATM 传输模式下的 G.SHDSL 接口。根据局端设备芯片类型不同，用户需选择不同的接口兼容能力，实现与局端设备的对接。AR G3 系列路由器支持的兼容性模式有探寻模式、厂家标识和互通模式，具体如表 3-35 所示。

表 3-35　AR G3 系列路由器支持的兼容性模式

兼容性模式	子分类
探寻模式	**normal** 表示标准探寻模式
	long 表示兼容基于 2.5.x 和 3.0.x 的 Globespan 的收发器探寻模式

（续表）

兼容性模式	子分类
厂家标识 Vendor ID	**normal** 表示保留设备的 Vendor ID（厂商 ID）的值
	gs 表示使用 Globespan 的 Vendor ID；**gs enhanced** 表示使用 Globespan 的增强 Vendor ID 【说明】在与使用 Globespan 的 Vendor ID 的局端设备对接时，局端发现对端不是自己厂商设备时会将对端设备强制下线。通过将 Vendor ID 设置为 Globespan 的 Vendor ID，可防止设备被强制下线。当配置使用 Globespan 的 Vendor ID 若与对端设备对接仍不成功时，可尝试使用 Globespan 的增强 Vendor ID 与对端设备进行对接
互通模式	**normal** 表示保留默认互通模式
	specific 表示在和 Globespan 的较低版本对接且速率低（小于 512 kbit/s）时，对端发送的信号功率谱密度不符合规范，通过设置物理层的互通模式为 specific，可以正确识别对端的信号

（10）（可选）配置 G.SHDSL 接口的信噪比

G.SHDSL 接口的信噪比仅支持工作在 ATM 传输模式下的 G.SHDSL 接口。AR G3 系列路由器可以配置以下两种 G.SHDSL 接口的信噪比。

① 当前上下行信噪比：当设备的实际信噪比值大于设定的信噪比值时，设备将激活成功。

② 最差上下行信噪比：当设备的最差信噪比值低于设定的信噪比值时，设备将直接掉线。

（11）（可选）使能 G.SHDSL 线路探询功能

使能线路探询功能，在线路激活过程中路由器将以最佳的线路速度进行激活，具体表现在以下两个方面。

① 如果局端配置的 G.SHDSL 线路的最大和最小速率不同，则线路的激活速率应在此范围内，否则无法激活，此时可通过使能线路探询功能，设备选择在此速率范围内且与实际线路最为匹配的速率激活。

② 如果局端配置的 G.SHDSL 线路的最大和最小速率相同，则线路的激活速率应为此固定速率，否则无法激活，此时可通过去使能线路探询功能，选择局端配置的固定速率激活。

（12）激活 G.SHDSL 接口

G.SHDS 接口去激活后，设备与局端建立通信的连接不再存在，如果要进行业务传输，则必须重新激活该接口。

3.14.3　配置 G.SHDSL 接口

当 G.SHDSL 线路上承载的是 ATM 信元时，G.SHDSL 接口要选择 ATM 模式进行配置，具体配置步骤如表 3-36 所示（注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序）；当需要 G.SHDSL 线路上承载的是以太网帧时，G.SHDSL 接口要选择 PTM 模式进行配置，具体配置步骤如表 3-37 所示（注意：其中的属性参数都有缺省配置，可根据实际需要选择配置，且没有严格的先后次序）。在 PTM 模式下，G.SHDSL 接口的单板能力、G.SHDSL 上行接口的兼容性模式和 G.SHDSL 接口的信噪比参数均不能在 G.SHDSL 接口上配置。但 G.SHDSL 上行接口所选择的传输模式均需要与局端设备的传输模式相同。

表 3-36 **ATM 模式下的 VDSL 接口配置步骤**

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
配置接口的传输模式	2	**set workmode slot** *slot-id* **shdsl atm** 例如：**set workmode slot** 1 **vdsl atm**	配置 G.SHDSL 接口工作在 ATM 模式。参数 *slot-id* 用来指定 G.SHDSL 接口所在的槽位号。执行该步骤后，需要重启单板并等待一段时间才能使配置生效 切换 G.SHDSL 接口的传输模式前，所有的 G.SHDSL 接口都必须去激活和解绑定 【说明】AR158E、AR158EVW 和 AR208E 的主控板仅有一个 WAN 物理接口，但可虚拟成 4 个 G.SHDSL 接口，接口编号从 8 到 11。一旦设置了单板的传输模式，这 4 个 G.SHDSL 接口都将工作在相同的传输模式 AR1200、AR2204、AR2220L、AR2220、AR2240 和 AR3200 使用的 4G.SHDSL 单板仅有一个物理接口，但可虚拟成 4 个 G.SHDSL 接口，接口序号从 0 到 3。一旦设置了单板的传输模式，这 4 个 G.SHDSL 接口都将工作在相同的传输模式 缺省情况下，G.SHDSL 接口工作在 PTM 模式下
去激活 G.SHDSL 接口	3	**interface atm** *interface-number* 例如：[Huawei] **interface atm 1/0/0**	进入 ATM 工作模式下的 G.SHDSL 接口视图，参数 *interface-number* 用来指定 ATM 工作模式下的 G.SHDSL 接口编号
	4	**shutdown** 例如：[Huawei-Atm1/0/0] **undo shutdown**	去激活 G.SHDSL 接口
配置接口的绑定	5	**shdsl bind m-pair** *link-number* 例如：[Huawei-Atm1/0/0] **shdsl bind m-pair** 3	配置指定 G.SHDSL 接口以 M-Pair 模式绑定。参数 *link-number* 用来指定绑定接口的数量，取值范围为 2～4 的整数。取值为 2：两接口可绑定接口的为 Port 0 和 Port 1 或 Port 2 和 Port 3；取值为 3：三接口可绑定接口的为 Port 0、Port 1 和 Port 2；取值为 4：四接口可绑定接口的为 Port 0、Port 1、Port 2 和 Port3 缺省情况下，G.SHDSL 接口未绑定任何模式 【说明】当设备工作在 CPE（客户端）模式下时，执行命令 **shdsl bind m-pair auto**，配置 G.SHDSL 接口以自动模式绑定，本端根据对端接口连线模式进行协商，最终协商的连线模式与对端配置一致 **绑定的接口必须是同一 4G.SHDSL 单板上的连续几个接口**，绑定的接口号必须从偶数（包括 0）开始，开始绑定的接口为主接口，被绑定的接口为从接口。但只有待绑定接口均处在去激活状态，且均没有配置业务时，才可配置接口绑定或解绑定 绑定成功后，同一绑定组内接口的传输标准、功率频谱密度模式、线路探询功能将恢复为缺省配置。如果要激活绑定接口或配置绑定接口的上行参数，只能在主接口上进行，其余接口的配置与主接口保持一致。例如，配置接口激活时，只需激活主接口，其他接口一起被激活。在 M-Pair 绑定模式下，当其中一个接口发生故障时，整个业务中断

（续表）

配置任务	步骤	命令	说明
配置接口的传输标准	6	**shdsl annex** { **a** | **all** | **b** } 例如：[Huawei-Atm1/0/0] **shdsl annex a**	配置 G.SHDSL 接口的传输标准，**但如果该接口处于 ATM 模式下的 M-Pair 绑定状态且不是主接口，那么该接口将无法配置传输标准**。命令中的选项说明如下。 • **a**：多选一选项，表示 G.SHDSL 接口支持的传输标准符合 G.991.2 Annex A 和 G.991.2 Annex F 标准。选择本选项后，当 G.SHDSL 接口线路实际净荷速率小于 2 304 kbit/s 时，设备将执行 G.991.2 Annex A 标准；当 G.SHDSL 接口线路实际净荷速率介于 2 304 kbit/s 和 5 696 kbit/s 之间时，设备将执行 G.991.2 Annex F 标准 • **b**：多选一选项，表示 G.SHDSL 接口支持的传输标准符合 G.991.2 Annex B 标准和 G.991.2 Annex G 标准。选择本选项后，当 G.SHDSL 接口线路实际净荷速率小于 2 304 kbit/s 时，设备将执行 G.991.2 Annex B 标准；当 G.SHDSL 接口传输速率介于 2 304 kbit/s 和 5 696 kbit/s 之间时，设备将执行 G.991.2 Annex G 标准 • **all**：多选一选项，表示 G.SHDSL 接口支持的传输标准同时支持 G.991.2 Annex A 和 G.991.2 Annex F 标准以及 G.991.2 Annex B 标准和 G.991.2 Annex G 标准。线路对接的两端将自适应进行选择 缺省情况下，G.SHDSL 接口的传输标准为 **all** 模式
配置接口的功率频谱密度模式	7	**shdsl psd** { **asymmetry** | **symmetry** } 例如：[Huawei-Atm1/0/0] **shdsl psd symmetry**	配置 G.SHDSL 接口的功率频谱密度模式。命令中的选项说明如下。 • **asymmetry**：二选一选项，指定 G.SHDSL 接口的 PSD（Power Spectral Density，功率频谱密度）模式为非对称模式。非对称 PSD 采用较高的发送功率来实现更佳的传输性能，适用于长距离传输 • **symmetry**：二选一选项，指定 G.SHDSL 接口的 PSD 模式为对称模式。对称 PSD 与其他的业务具有良好的频谱兼容性，消耗的功率也更低，适用于短距离传输 缺省情况下，G.SHDSL 接口的功率频谱密度模式为对称模式
配置接口的发射功率	8	**shdsl pbo auto** 例如：[Huawei-Atm1/0/0] **shdsl pbo auto**	（二选一）正常情况下，配置接口会根据线路噪声情况，自动调整发送功率 缺省情况下，G.SHDSL 接口选择自动调节发送功率方式
		shdsl pbo *value* 例如：[Huawei-Atm1/0/0] **shdsl pbo** 10	（二选一）当线路的噪声已知的情况下，或者自动调整不准确的时候，手动调整发射功率。参数用来指定发送功率调节值，取值范围为 1～31 dB
配置接口单板能力（**仅 ATM 模式下可配置**）	9	**shdsl capability** { **auto** | **g-shdsl** | **g-shdsl.bis** } 例如：[Huawei-Atm1/0/0] **shdsl capability g-shdsl.bis**	配置 G.SHDSL 接口的单板能力。命令中的选项说明如下。 • **auto**：多选一选项，指定 G.SHDSL 接口单板能力为自动模式 • **g-shdsl**：多选一选项，指定 G.SHDSL 接口单板能力为 g-shdsl 模式 • **g-shdsl.bis**：多选一选项，指定 G.SHDSL 接口单板能力为 g-shdsl.bis 模式 如果在同一个 G.SHDSL 接口视图下重复执行 **shdsl capability** 命令时，新配置将覆盖老配置 缺省情况下，G.SHDSL 接口的单板能力为 auto 模式

（续表）

配置任务	步骤	命令	说明
配置接口单板能力（仅 ATM 模式下可配置）	10	**shdsl pam** { **16** | **32** | **auto** } 例如：[Huawei-Atm1/0/0] **shdsl pam 32**	配置 G.SHDSL 接口调制模式。命令中的选项说明如下。 • **16**：多选一选项，指定 G.SHDSL 接口的调制模式为 16 PAM • **32**：多选一选项，指定 G.SHDSL 接口的调制模式为 32 PAM • **auto**：多选一选项，指定 G.SHDSL 接口的调制模式为自动模式 【说明】g.shdsl 能力模式仅支持 16 PAM 调制模式，g.shdsl.bis 能力支持 16 PAM 模式和 32 PAM 模式以及 auto 模式 缺省情况下，G.SHDSL 接口调制模式为 auto 模式
	11	**shdsl bind m-pair 2 pairs** { **auto-enhanced** | **enhanced** | **standard** } 例如：[Huawei-Atm1/0/0] **shdsl bind m-pair 2 pairs enhanced**	配置 G.SHDSL 接口绑定可选增强模式。命令中的选项说明如下。 • **auto-enhanced**：多选一选项，指定 G.SHDSL 接口绑定为自适应增强模式 • **enhanced**：多选一选项，指定 G.SHDSL 接口绑定为增强模式 • **standard**：多选一选项，指定 G.SHDSL 接口绑定为标准模式 缺省情况下，G.SHDSL 接口绑定模式为 auto-enhanced 模式 【说明】g.shdsl 能力模式仅支持 enhanced 模式；g.shdsl.bis 能力模式支持 enhanced 模式、standard 模式和 auto-enhanced 模式，缺省配置为 auto-enhanced 模式 对于 AR1200、AR2204、AR2220L、AR2220、AR2240 和 AR3200 系列，本命令仅支持在接口序号为 0 或 2 的接口下进行配置；对于 AR158E、AR158EVW 和 AR208E 系列，本命令仅支持在接口序号为 8 或 10 的接口下进行配置
	12	**shdsl rate maximum** *maximum* 例如：[Huawei-Atm1/0/0] **shdsl rate maximum** 2000 例如：[Huawei-Atm1/0/0] **shdsl rate maximum** 5696	配置 G.SHDSL 接口手动设置速率的最大值，参数 *maximum* 的取值范围为 192～5 696 kbit/s。G.SHDSL 接口单板能力为 g-shdsl.bis 模式时，取值范围为 192～5 696，G.SHDSL 接口单板能力为 g-shdsl 模式时，取值范围为 192～2 304 手动配置 G.SHDSL 接口最大传输速率必须大于等于手动配置 G.SHDSL 接口最小传输速率 【说明】参数 *maximum* 的粒度是 64 kbit/s（2 312 kbit/s 和 3 848 kbit/s 除外），比如当该值设为 650 kbit/s 时，此配置按 640 kbit/s 生效；当该值设为 2 312 kbit/s 时，此配置按照 2 312 kbit/s 生效
	13	**shdsl rate minimum** *minimum* 例如：[Huawei-Atm1/0/0] **shdsl rate minimum** 2000	配置 G.SHDSL 接口手动设置速率的最小值，参数取值及说明参见上一步的 **shdsl rate maximum** 说明

（续表）

配置任务	步骤	命令	说明
配置接口的兼容性模式（仅 ATM 模式下可配置）	14	**shdsl compatibility pmms { normal | long } vendor {normal | gs [enhanced]} filter { normal | specific }** 例如：[Huawei-Atm1/0/0] **shdsl compatibility pmms long vendor gs filter specific**	配置 G.SHDSL 接口的兼容性模式。命令中的选项说明如下。 • **pmms { normal | long }**：指定 G.SHDSL 接口探寻模式：**normal** 选项表示标准探寻模式；**long** 选项表示兼容基于 2.5.x 和 3.0.x 的 Globespan 的收发器探寻模式 • **vendor { normal | gs [enhanced]}**：指定 G.SHDSL 接口的厂商标识 Vendor ID：**normal** 选项表示使用设备的 Vendor ID；**gs** 选项表示使用 Globespan 的 Vendor ID，**gs enhanced** 可选项表示使用 Globespan 的增强 Vendor ID • **filter { normal | specific }**：指定 G.SHDSL 接口的互通模式：**normal** 选项表示使用默认互通模式；**specific** 选项表示在和 Globespan 的较低版本对接且速率低（<512 kbit/s）时，对端发送的信号功率谱密度不符合规范，通过设置物理层的互通模式为 specific，可以正确识别对端的信号 缺省情况下，G.SHDSL 接口的兼容性模式使用 **normal** 模式
（可选）配置接口信噪比（仅 ATM 模式下可配置）	15	**shdsl current target snr margin upstream** *value* 例如：[Huawei-Atm1/0/0] **shdsl current target snr margin upstream** 8	配置 G.SHDSL 接口当前上行信噪比，参数 *value* 的取值范围为 0～10 dB，取整数 缺省情况下，G.SHDSL 接口的当前上行信噪比取值为 6 dB 如果在同一个 G.SHDSL 接口视图下重复执行本命令时，新配置将覆盖老配置
	16	**shdsl current target snr margin downstream** *value* 例如：[Huawei-Atm1/0/0] **shdsl current target snr margin downstream** 5	配置 G.SHDSL 接口当前下行信噪比，参数 *value* 的取值范围为 0～10 dB，取整数；下行值要比上行值小 缺省情况下，G.SHDSL 接口的当前下行信噪比取值为 6 dB 如果在同一个 G.SHDSL 接口视图下重复执行本命令时，新配置将覆盖老配置
	17	**shdsl worst case target snr margin upstream** *value* 例如：[Huawei-Atm1/0/0] **shdsl worst case target snr margin upstream** 5	配置 G.SHDSL 接口最差上行信噪比，参数 *value* 的取值范围为 0～6 dB，取整数 缺省情况下，G.SHDSL 接口的最差上行信噪比取值为 0 dB 如果在同一个 G.SHDSL 接口视图下重复执行本命令时，新配置将覆盖老配置
	18	**shdsl worst case target snr margin downstream** *value* 例如：[Huawei-Atm1/0/0] **shdsl worst case target snr margin downstream** 3	配置 G.SHDSL 接口最差下行信噪比，参数 *value* 的取值范围为 0～6 dB，取整数；下行值要比上行值小 缺省情况下，G.SHDSL 接口的最差下行信噪比取值为 0 dB 如果在同一个 G.SHDSL 接口视图下重复执行本命令时，新配置将覆盖老配置
（可选）使能线路探询功能	19	**shdsl line-probing enable** 例如：[Huawei-Atm1/0/0] **shdsl line-probing enable**	使能 G.SHDSL 接口的线路探询功能 缺省情况下，已使能线路探询功能，可用 shdsl line-probing **disable** 命令去使能线路探询功能。不论使能或去使能线路探询功能，一旦线路激活失败，局端需重新配置线路的最大和最小速率，以保证线路激活成功

（续表）

配置任务	步骤	命令	说明
（可选）使能线路探询功能	19	**shdsl line-probing enable** 例如：[Huawei-Atm1/0/0] **shdsl line-probing enable**	【说明】出现如下场景时，使用此命令 若局端配置了G.SHDSL线路的最大和最小速率不同，则线路的激活速率应在此范围内，否则无法激活，此时可通过使能线路探询功能，设备选择在此速率范围内且与实际线路最为匹配的速率激活 若局端配置了G.SHDSL线路的最大和最小速率相同，则线路的激活速率应为此固定速率，否则无法激活，此时可通过去使能线路探询功能，选择局端配置的固定速率激活 如果该接口处于ATM传输模式下的M-Pair绑定状态且不是主接口，则无法去使能或使能线路探询功能
激活G.SHDSL接口	20	**undo shutdown** 例如：[Huawei-Atm1/0/0] **undo shutdown**	激活G.SHDSL接口 G.SHDSL接口去激活后，设备与局端建立通信的连接不再存在，如果要进行业务传输，则必须重新激活该接口，以使以上G.SHDSL接口的上行线路参数配置生效

表 3-37　　PTM 模式下的 VDSL 接口配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
配置接口的传输模式	2	**set workmode slot** *slot-id* **shdsl ptm** 例如：**set workmode slot 1 vdsl atm**	配置G.SHDSL接口工作在PTM模式。其他说明参见前面表3-36中的第2步
去激活G.SHDSL接口	3	**interface Ethernet** *interface-number* 例如：[Huawei] **interface ethernet 1/0/0**	进入PTM工作模式下的G.SHDSL接口视图，参数*interface-number*用来指定PTM工作模式下的G.SHDSL接口编号
	4	**shutdown** 例如：[Huawei-Ethernet1/0/0] **undo shutdown**	去激活G.SHDSL接口
配置接口的绑定	5	**shdsl bind efm** *link-number* 例如：[Huawei-Ethernet1/0/0] **shdsl bind efm** 3	配置指定G.SHDSL接口以EFM模式绑定 【说明】当G.SHDSL接口工作在PTM模式下，可使用EFM模式绑定接口。在EFM模式下，支持最多4个接口的绑定，绑定后的速率为各接口的速率之和 如果要激活以EFM模式绑定的G.SHDSL接口，那么主从接口上都必须配置激活，并且需先激活主接口，再激活从接口 绑定成功后，同一绑定组内各个接口的参数均可配置，且可配置不同的参数。例如，同一绑定组内各个接口可配置不同的传输标准。在EFM绑定模式下，当其中一个接口发生故障时，业务自动分流到其他接口上，业务流量小于接口实际带宽时业务不中断。且当G.SHDSL接口以EFM模式绑定成功后，不能再被其他接口绑定。例如，接口1/0/0与接口1/0/1绑定之后，接口1/0/2不能再次与接口1/0/0和接口1/0/1进行绑定 其他说明参见前面表3-36中的第5步

（续表）

配置任务	步骤	命令	说明
配置接口的传输标准	6	**shdsl annex** { **a** | **all** | **b** } 例如：[Huawei-Ethernet1/0/0] **shdsl annex a**	配置 G.SHDSL 接口的传输标准。其他说明参见前面表 3-36 中的第 6 步
配置接口的功率频谱密度模式	7	**shdsl psd** { **asymmetry** | **symmetry** } 例如：[Huawei-Ethernet1/0/0]**shdsl psd symmetry**	配置 G.SHDSL 接口的功率频谱密度模式。其他说明参见前面表 3-36 中的第 7 步
配置接口的发射功率	8	**shdsl pbo auto** 例如：[Huawei-Ethernet1/0/0] **shdsl pbo auto**	（二选一）其他说明参见前面表 3-36 中的第 8 步
		shdsl pbo *value* 例如：[Huawei-Ethernet1/0/0]**shdsl pbo** 10	
（可选）使能线路探询功能	9	**shdsl line-probing enable** 例如：[Huawei-Ethernet1/0/0]**shdsl line-probing enable**	使能 G.SHDSL 接口的线路探询功能。其他说明参见前面表 3-36 中的第 19 步
激活 G.SHDSL 接口	10	**undo shutdown** 例如：[Huawei-Ethernet1/0/0]**undo shutdown**	激活 G.SHDSL 接口 G.SHDSL 接口去激活后，设备与局端建立通信的连接不再存在，如果要进行业务传输，则必须重新激活该接口，以使以上 G.SHDSL 接口的上行线路参数配置生效

可使用 **display dsl interface** { **atm** | **ethernet** } *interface-number* 命令查看 G.SHDSL 接口的状态信息，包括 G.SHDSL 接口的链路状态信息、厂家信息和性能统计信息。

3.14.4　G.SHDSL 接口上行配置示例

本示例基本网络结构如图 3-35 所示，企业 A 希望运营商提供一种部署简单、上下行方向均要求高速的数据接入方式，以满足各种业务需求，如安全、VPN、视频会议。另外，企业 A 发现当前的带宽无法满足其数据传输需求，希望运营商提供更大的带宽。

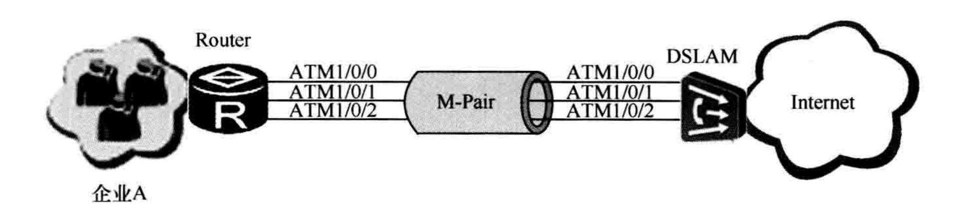


图 3-35　G.SHDSL 接口上行配置示例基本网络结构

根据 3.14.2 小节介绍的配置任务和 3.14.3 小节介绍的配置可以得出本示例的基本配置思路如下。

① 根据局端的 G.SHDSL 接口传输模式，在设备的 G.SHDSL 接口上配置相同的传输模式。

② 配置 G.SHDSL 参数前，去激活 G.SHDSL 接口，然后配置 G.SHDSL 上行参数，以获得 G.SHDSL 线路的最佳使用效果。上行参数包括接口绑定、传输标准、功率频谱密

度模式、线路探询，除线路探询外的参数需与局端配置的参数保持一致，否则线路无法激活。

③ 最后激活 G.SHDSL 接口，使配置生效，然后就可以在 G.SHDSL 线路上传输业务了。

在此仅以 ATM 传输模式下的 G.SHDSL 接口为例进行介绍。具体配置步骤如下。

① 配置设备的 G.SHDSL 接口传输模式为 ATM。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] set workmode slot 1 shdsl atm
Changing the working mode will reset the board in slot 1. Continue? [y/n]:y
INFO: Resetting board[1] succeeded.
```

② 去激活 G.SHDSL 接口。这里要注意，因为后面为了实现更高的带宽，要进行多个 G.SHDSL 接口绑定，所以这里要分别对这些 G.SHDSL 接口进行去激活操作（其中 ATM1/0/0 接口为主接口）。

```
[Router] interface atm 1/0/0
[Router-Atm1/0/0] shutdown
[Router-Atm1/0/0] quit
[Router] interface atm 1/0/1
[Router-Atm1/0/1] shutdown
[Router-Atm1/0/1] quit
[Router] interface atm 1/0/2
[Router-Atm1/0/2] shutdown
[Router-Atm1/0/2] quit
```

③ 配置必要的 G.SHDSL 上行参数，要与局端设备配置一致。

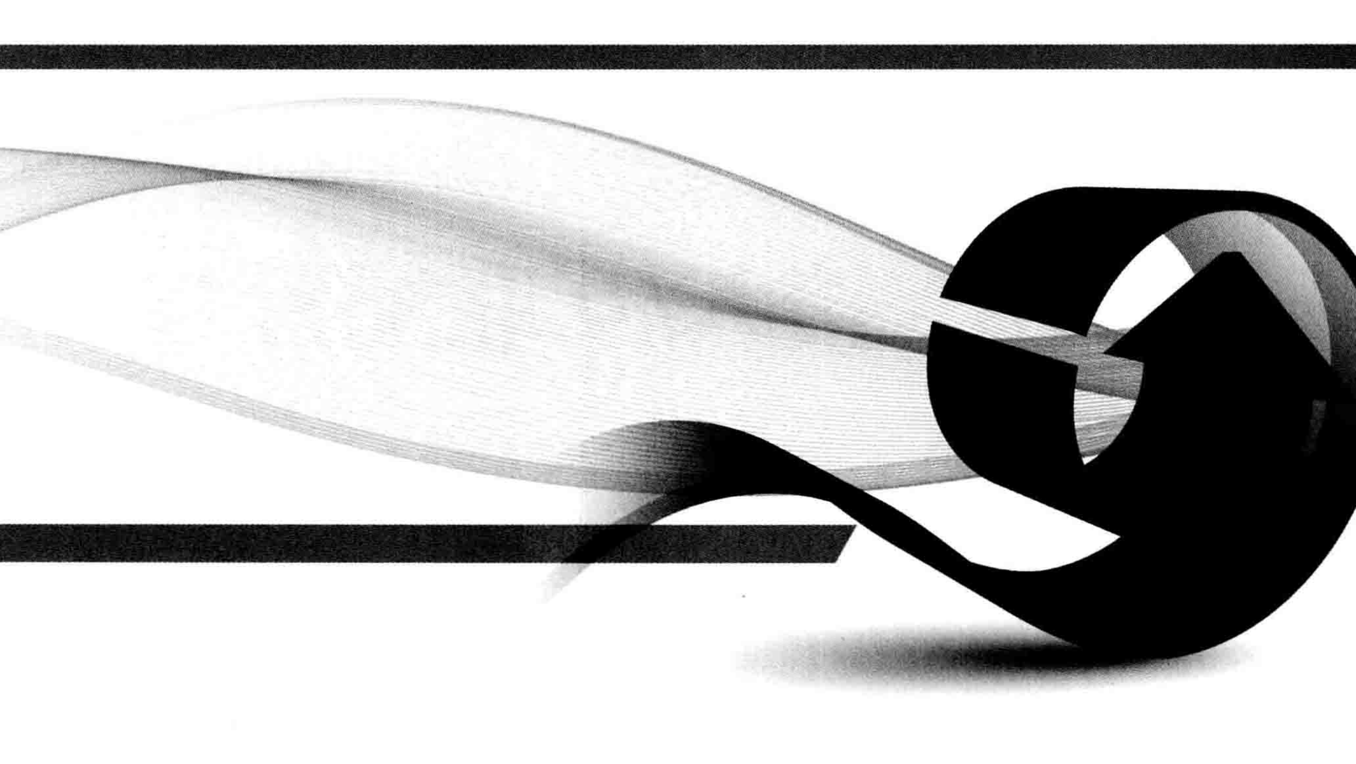
```
[Router] interface atm 1/0/0
[Router-Atm1/0/0] shdsl bind m-pair 3            !—配置 G.SHDSL 接口以 M-Pair 进行 3 接口绑定
[Router-Atm1/0/0] shdsl annex b                  !—配置 ATM1/0/0 的传输标准为 G.991.2 Annex B
[Router-Atm1/0/0] shdsl psd symmetry             !—配置 ATM1/0/0 的功率频谱密度模式为对称模式
[Router-Atm1/0/0] shdsl line-probing enable      !—使能 ATM1/0/0 的线路探询功能
```

④ 激活主接口 ATM1/0/0（被绑定的子接口也随之被激活）

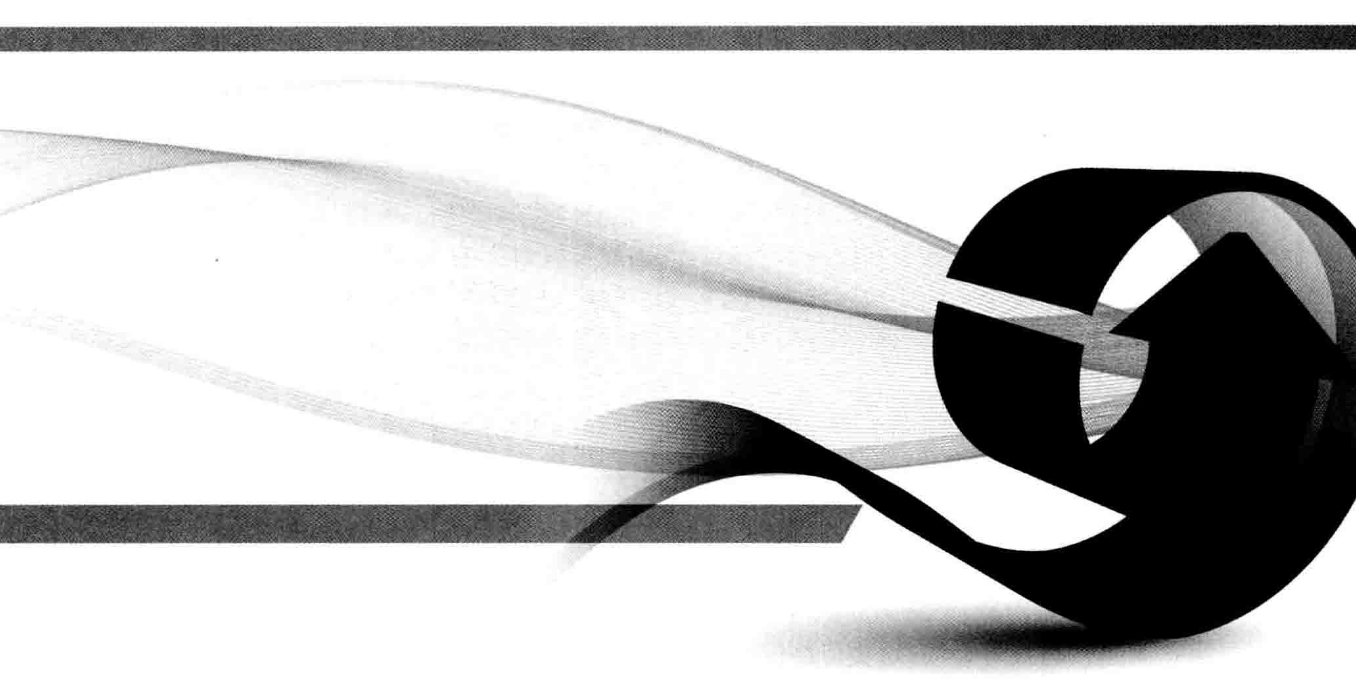
```
[Router-Atm1/0/0] undo shutdown
[Router-Atm1/0/0] quit
```

配置好后，可通过 **display dsl interface atm** 1/0/0 命令查看设备的 G.SHDSL 接口是否激活、上行参数是否配置正确，也可使用 **display interface atm** 1/0/0 命令查看设备的 G.SHDSL 接口的状态信息。具体输出示例略。

说明 在本章 3.1.1 小节介绍的 AR G3 系列路由器所支持的逻辑接口类型中，大部分已在配套的《华为交换机学习指南》一书中作了介绍，如 VLANIF 接口、以太网子接口、Eth-Trunk 接口、Loopback 接口、NULL 接口等，而像 VT、MP-Group、Dialer 这些常用的逻辑接口在本书第 4 章将有比较多的涉及(其实它们的配置就是创建和分配 IP 地址这两个方面，很简单)，故均不在本章重复介绍。



第4章 WAN接入/互联配置与管理



由于路由器主要用于WAN接入与互联，所以学习和掌握路由器的WAN接入与互联配置方法就成了学习路由器配置与管理的基础内容。

在路由器的WAN接入与互联中主要包括两大类：一是专线方式的接入或互联，如通过E1或T1之类的专线接入与互联；还有一种就是按需拨号方式，这种方式不是永久连接的，如ISDN、ADSL、VDSL等拨号方式。专线接入方式的配置比较简单，只须按照本书第3章介绍的方法配置好链路两端的对应物理接口即可，而按需拨号方式则不是这么简单了，还需要配置拨号接口属性和相应的链路层协议（包括协议封装、认证和协议参数等）。

本章将重点介绍AR G3系列路由器中按需拨号的DCC（包括轮询DCC和共享DCC）以及在WAN接入与互联中广泛应用的PPP、MP以及PPPoE协议的配置与管理方法。其中的重点与难点是DCC与PPPoE的配置。

4.1 广域网接入/互联网概述

广域网接入/互联是指通过接入广域网线路（主要是指 Internet 线路），如 Modem、ISDN、ADSL、VDSL、G.SHDSL 等有线拨号或者专线线路（如 E1、T1 线路），以及像 3G 无线接入线路，或者通过专门的广域网络（如 SONET/SDH 传输网、EPON/GPON 传输网等），实现远程设备或者网络间的广域网接入与互联。

在第 3 章介绍了用于各种广域网接入/互联的 WAN 接口，根据它们的接入/互联方式可以分为两大类：一类是属于专线接入型的，只需配置好对应的 WAN 接口即可，如通过 E1、T1、光纤专线进行的广域网接入与互联的 CE1/PRI、E1-F、CT1/RPI、T1-F、POS、CPOS、PON 等接口。这类广域网接入/互联基本网络结构如图 4-1 所示。



图 4-1 专线型广域网接入/互联基本网络结构

另一类是按需拨号型的。这类广域网接入/互联仅配置好对应的 WAN 接口是不够的，还需要配置拨号接口和账户属性，如通过 ISDN、ADSL、VDSL、G.SHDSL 和 3G 无线线路进行的 PRI 接口、ADSL 接口、VDSL 接口、G.SHDSL 接口和 3G Cellular 接口（说明：ISDN、ADSL、VDSL、G.SHDSL 等也有专线接入方式，光线接入也有拨号方式）。图 4-2 所示为 xDSL（包括 ADSL、VDSL 和 G.SHDSL）拨号广域网接入/互联方式的基本网络结构。

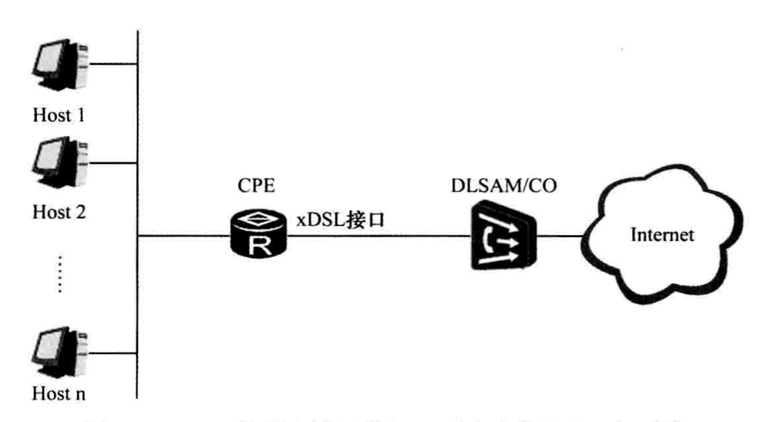


图 4-2 xDSL 拨号广域网接入/互联方式的基本网络结构

对于专线接入型没什么额外介绍的，仅通过本书第 3 章介绍的对应 WAN 接口配置就可以实现对应广域网线路的接入与互联。本章介绍的是按需拨号型的广域网接入与互联的配置与管理方法。在华为 AR G3 系列路由器中，各种拨号服务采用的是 DCC（Dial Control Center，拨号控制中心）集中管理方式。各种按需拨号方式的总体配置任务包括如下两个方面。

（1）配置各种报号服务所对应的 WAN 接口

这方面的 WAN 接口包括 Serial 接口、ADSL 接口、VDSL 接口、G.SHDSL 接口和 3G Cellular 接口，具体配置参见本书第 3 章的相应介绍。

（2）（可选）配置 DCC

DCC 的作用就是配置各种拨号服务所需的拨号接口及其账户和链路属性。当然，拨号接口和拨号属性也可在特定的拨号接入方式下配置，只不过此时它没有 DCC 中的一些特定功能，如轮询拨号、多物理线路共享拨号属性、动态线路备份等。

（3）（可选）配置各种 WAN 接口链路所封装的链路层协议

在广域网接入/互联中，各种 WAN 拨号接口所封装的链路层协议主要包括 PPP、MP（多 PPP）和 PPPoE 这三种点对点协议。因为串行链路都有缺省的链路协议封装和参数配置，所以仅需根据实际需要选择配置。

4.2 DCC 基础

DCC（拨号控制中心）是指路由器之间通过 ISDN 网络、xDSL 网络、3G 网络、PSTN 网络等进行互联，或者路由器作为 PPPoE/PPPoEoA/PPPoA 客户端与 PPPoE/PPPoEoA/PPPoA 服务器之间互联时采用的技术，主要提供按需拨号服务。

4.2.1 DCC 概述

当需要传送的信息具有时间不确定性、突发性、总体数据量小等特点时，采用仅在有数据需要传送时才建立连接并通信的方式是最经济的一种接入方式，也称“按需拨号”方式，如我们家庭中最常用的普通 Modem、ADSL 拨号接入。

所谓“按需拨号”是指跨 ISDN 网络、3G 网络、PSTN 网络等相连的路由器之间，或者路由器作为 PPPoE/PPPoEoA/PPPoA 客户端与 PPPoE/PPPoEoA/PPPoA 服务器（通常位局于局端）之间不预先建立连接，而是当它们之间有数据需要传送时才启动拨号流程，以拨号的方式建立连接并传送信息。当链路空闲时又会自动断开拨号连接。在 AR G3 系列路由器中，DCC 正是这样一种控制按需拨号的技术，可广泛应用于各种拨号接入方式，如 Modem、ISDN、ADSL、VDSL、G.SHDSL 和无线 3G 等。

AR G3 系列路由器支持两种 DCC，即“轮询 DCC”（Circular DCC，C-DCC）和“共享 DCC”（Resource-Shared DCC，RS-DCC）。这里首先要明白什么是“轮询”，什么是“共享”。“轮询”的意思是在本端多个接口需要向多个目的地址发起呼叫时，依据为各物理接口配置的优先级从高到低选择由哪个接口建立呼叫；而“共享”是指去往同一个目的网络的所有拨号呼叫使用同一个拨号属性集，无需为每个拨号的物理接口单独配置拨号参数。

在正式介绍 DCC 的原理之前先介绍几个 DCC 配置术语，以方便用户理解 DCC。

1. 物理接口

实际存在的物理接口，如 ISDN BRI、ISDN PRI、ADSL 接口、VDSL 接口、Cellular 接口等。

2. Dialer 接口

“Dialer 接口”是为了配置 DCC 参数而设置的逻辑接口。物理接口可以通过绑定到 Dialer 接口而继承 DCC 配置信息。

3. 拨号接口

“拨号接口”是对拨号连接接口的泛称，可以是 Dialer 接口，也可以是捆绑到 Dialer 接口的物理接口，或者是直接配置 DCC 参数的物理接口。

4.2.2 两种 DCC 的拨号控制原理

本节将分别介绍 AR G3 系列路由器支持的“轮询 DCC”和“共享 DCC”两种 DCC 的基本拨号控制原理。

1. 轮询 DCC

在轮询 DCC 和共享 DCC 中，物理接口与 Dialer 接口的对应关系是不一样的。轮询 DCC 中物理接口与 Dialer 接口的对应关系有图 4-3 所示的几种。

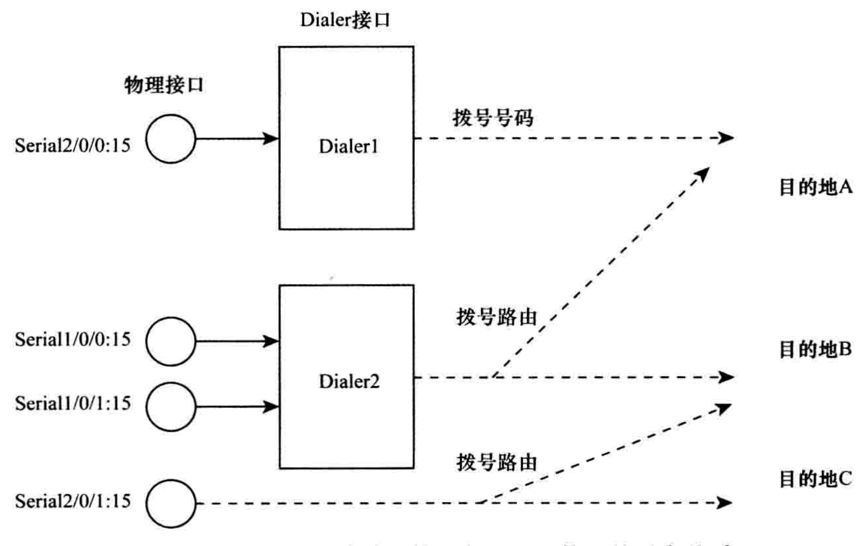


图 4-3 轮询 DCC 中物理接口与 Dialer 接口的对应关系

从图中可以得出轮询 DCC 具有以下特点。

① 一个 Dialer 接口中可以捆绑多个物理接口（如 Dialer2 中包括了两个物理接口），所有物理接口都继承同一个 Dialer 接口的属性。而任意一个物理接口只能属于一个 Dialer 接口，即一个物理接口只能服务于一种拨号服务，或者说一个物理接口只提供一种拨号服务。但物理接口也可以不属于任何 Dialer 接口（如 Serial1/0/1:15），而直接通过拨号路由（通过 **dialer route** 命令）方式映射到一个或多个目的地址。

② 一个 Dialer 接口可以通过配置多个拨号路由 **dialer route** 命令对应多个呼叫目的地址，也可以配置 **dialer number** 命令对应单个呼叫目的地址。

③ 如果仅访问一个目的地址，则可以直接在物理接口上配置 DCC 参数，但如果要访问多个目的地址，则必须要借助拨号循环组（Dialer Circular Group）把对应物理接口绑定到 Dialer 接口来继承 DCC 参数。当然，在仅访问一个目的地址时，也可以通过拨

号循环组把对应的物理接口绑定到 Dialer 接口来继承 DCC 参数。

总地来说，如果使用 Dialer 接口（单一目的地址时也可不使用 Dialer 接口），同一物理接口仅能属于一个 Dialer 接口；每个 Dialer 接口可以包含多个物理接口，每个 Dialer 接口可以对应一个或多个目的地址。即轮询 DCC 中的物理接口与 Dialer 接口可以是一对一，或者多对一关系，且一个 Dialer 接口可以配置一个或多个目的地址的拨号参数。

因为轮询 DCC 中的一个 Dialer 接口可以配置对应多个目的地址，所以轮询 DCC 主要适用于物理链路较多、连接情况复杂的大中型站点。

2. 共享 DCC

共享 DCC 中不同的 Dialer 接口可以实现共享同一个物理拨号链路，实现在不同的拨号中，同一个物理拨号链路使用不同的工作参数。物理链路工作参数的切换自动根据连接来决定，不需要管理员的干预。因此共享 DCC 主要适用于可用物理链路较少，但连接需求较多的中小型站点。

共享 DCC 中的物理接口、Dialer bundle（拨号捆绑）与 Dialer 接口的对应关系如图 4-4 所示。由于实现了逻辑配置和物理配置的相互分离，共享 DCC 比轮询 DCC 简单，并具有良好的灵活性。

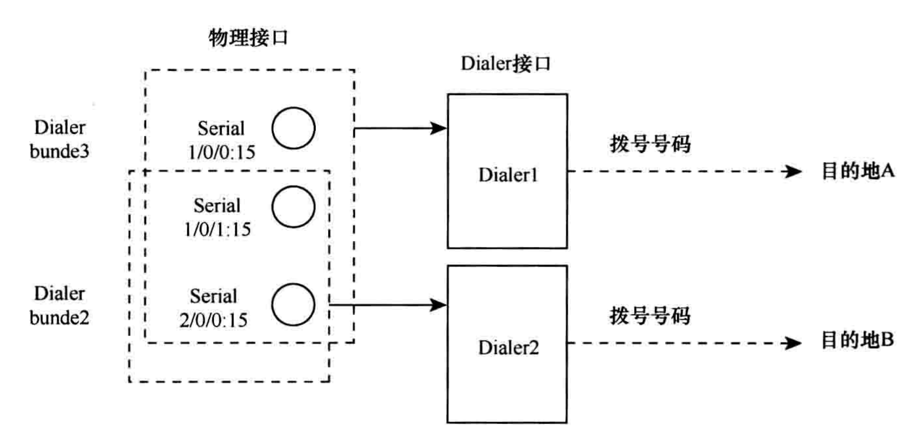


图 4-4　共享 DCC 的物理接口、Dialer bundle 和 Dialer 接口对应关系

从图中可以得出共享 DCC 具有以下特点。

① 将物理接口的配置与呼叫的逻辑配置分开进行，再将两者动态地捆绑起来，从而可以实现相同物理接口为多种不同拨号应用服务的目的。

② 一个 Dialer 接口可以捆绑多个物理接口，同时任意一个物理接口也可属于多个 Dialer 接口，**即一个物理接口可以提供多种拨号服务**。使用共享属性集（RS-DCC set，包括 Dialer 接口、Dialer bundle 和物理接口等参数）来描述拨号属性，去往同一个目的网络的所有拨号呼叫使用同一个共享属性集。

③ 一个 Dialer 接口**只能对应一个呼叫目的地址**，因为是直接使用 **dialer number** 命令配置对应的单个呼叫目的地址，而不能使用拨号路由 **dialer route** 命令配置对应的多个呼叫目的地址。

④ 在物理接口上**不能直接配置共享 DCC 参数**，物理接口必须通过绑定到 Dialer 接口才能实现共享 DCC 拨号功能。

从以上特点可以看出，在共享 DCC 方式下，同一物理接口可以属于多个 Dialer 捆绑，并进而服务于多个 Dialer 接口。每个 Dialer 接口只能使用一个 Dialer 捆绑，同时也只能设置一个目的地址。但同一个 Dialer 捆绑中的物理接口可以有不同的优先级，Dialer 捆绑对应的 Dialer 口可以根据优先级选择呼叫时使用的物理接口。相同的物理接口在不同的 Dialer 捆绑中可以有不同的优先级。

总体来说就是，向同一个目的地址进行拨号的物理接口可以形成一个捆绑，然后与唯一的一个 Dialer 接口对应；如果一个物理接口需要向多个目的地址进行拨号，则需要加入多个捆绑，并且要对应不同的 Dialer 接口，因为此时每个 Dialer 接口只能对应一个目的地址。

对于共享 DCC 来说，因为物理接口属性和 DCC 参数配置是逻辑分开的，一组物理接口可以共享相同的 DCC 参数，具有配置简单的特点，且一个 Dialer 接口只能配置单一目的地址，所以适用于可用物理链路较少，但连接需求较多的中小型站点。

3. 轮询 DCC 和共享 DCC 的综合比较

如果要对轮询 DCC 和共享 DCC 的主要特点进行综合比较的话，可以用表 4-1 概括。

表 4-1 轮询 DCC 和共享 DCC 综合比较

比较选项	轮询 DCC	共享 DCC
物理接口与 Dialer 接口的对应关系	一个 Dialer 接口都可以有多个物理接口为它服务，**但任意一个物理接口只能属于一个 Dialer 接口**，即一个物理接口只能提供一种拨号服务	一个 Dialer 接口都可以有多个物理接口为它服务，**但任意一个物理接口可属于多个 Dialer 接口**，即一个物理接口可以提供多种分属于不同 Dialer 接口的拨号服务
目的地址	一个 Dialer 接口可以配置**一个或多个呼叫目的地址**	一个 Dialer 接口只能配置**一个呼叫目的地址**，即一个 Dialer 接口中的多物理接口共享一组拨号串
DCC 参数配置	物理接口既可以借助拨号循环组绑定到 Dialer 接口来继承 DCC 参数，**又可以直接配置 DCC 参数**	在物理接口上**不能直接配置共享 DCC 参数**，必须通过绑定到 Dialer 接口才能实现共享 DCC 拨号功能
拨号属性共享	服务于**同一个拨号循环组中的所有物理接口都共享同一个 Dialer 接口的属性**	使用共享属性集来描述拨号属性，**去往同一个目的网络的所有呼叫使用同一个共享属性集**
应用场景	适用于物理链路较多，连接情况复杂的大中型站点	适用于可用物理链路较少，但连接需求较多的中小型站点

4.2.3 DCC 的主要应用场景

DCC 主要应用于以下两种场景。

① 以备份形式为主干线路通信提供保障：在主干线路因为线路或其他原因出现故障而不能正常通信时，提供替代的辅助通路，确保业务正常进行。

一般来讲，用户是通过与现有网络不同的网络进行备份的，比如通过 ISDN 网络备份 IP 网络中的主干线路链路。设备提供备份功能时，支持两种备份方式：通过接口备份实现；通过动态路由备份实现。

② 当路由器作为 PPPoE/PPPoEoA/PPPoA 客户端时，DCC 通过按需拨号的功能，为用户节省费用。

1. 通过接口备份实现主干线路通信备份

图 4-5 所示为通过接口备份实现主干线路通信备份示例的基本网络结构。Dialer1 接口是拨号接口，用来备份物理接口 GE1/0/0 的主干线路连接。当接口 GE1/0/0 因故障不能传输数据时，接口上的所有流量会切换到与 Dialer1 接口绑定的 PRI2/0/0:15 接口上。此时流量会触发 DCC 拨号，从而实现使用 ISDN 网络备份主干线路通信的目的。

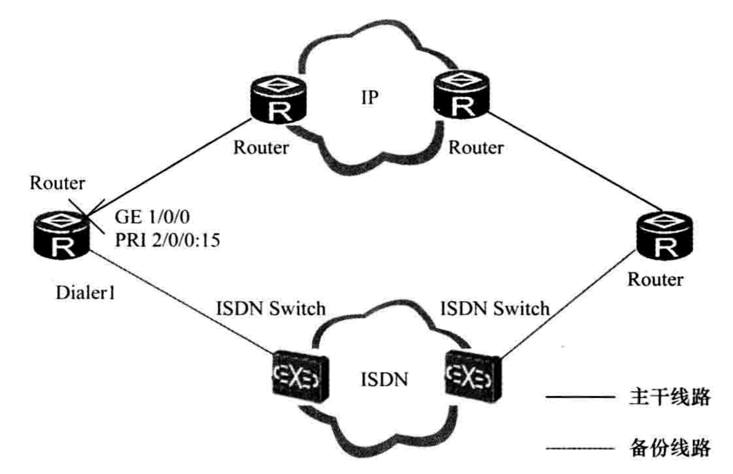


图 4-5　通过接口备份实现主干线路通信备份示例的基本网络结构

2. 通过动态路由备份实现主干线路通信备份

图 4-6 所示为通过动态路由备份实现主干线路通信备份示例的基本网络结构。当 RouterA 到 RouterB 的 10.10.10.1/24 网段没有有效路由时，RouterA 的 Dialer1 拨号接口会启动 DCC 拨号，从而实现使用 ISDN 网络备份主干线路通信。

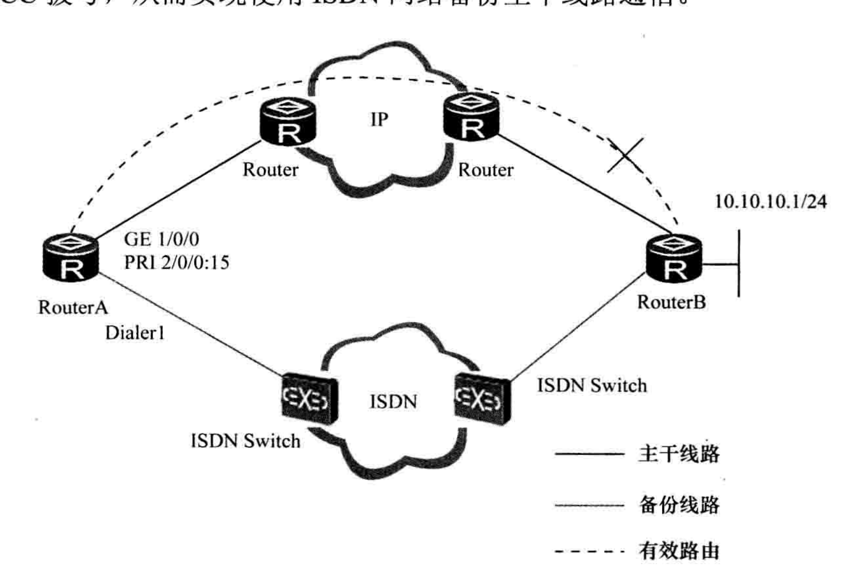


图 4-6　通过动态路由备份实现主干线路通信备份示例的基本网络结构

3. 路由器作为 PPPoE 客户端时的按需拨号

路由器作为 PPPoE 客户端时的按需拨号的基本网络结构如图 4-7 所示。在拨号连接

已经建立的情况下，当 PPPoE 客户端到 PPPoE 服务器之间没有流量时，PPPoE 客户端启用闲时断开功能将连接断开。一旦 PPPoE 客户端到 PPPoE 服务器再有流量，会触发 DCC 拨号并建立连接。

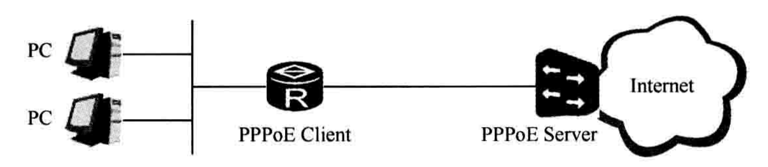


图 4-7 路由器作为 PPPoE 客户端时的按需拨号的基本网络结构

如果路由器作为 PPPoEoA/PPPoA 客户端，组网时还需要通过 DSLAM 设备接入 PPPoEoA/PPPoA 服务器。用于该场景的 DCC 必须是共享 DCC。

4.2.4 配置 DCC 前的准备

AR G3 系列路由器支持 ISDN PRI 接口、ADSL 接口、G.SHDSL 接口、VDSL 接口、E1-IMA 接口、WAN 侧以太网接口、ISDN BRI 接口、Async 接口、3G Cellular 接口用于 DCC 特性。但它们所支持的 DCC 特性并不完全一样。

① ADSL 接口、G.SHDSL 接口、VDSL 接口、E1-IMA 接口、WAN 侧以太网接口**只能用于共享 DCC** 实现设备作为 PPPoE/PPPoEoA/PPPoA 客户端时的按需拨号。

② Async 接口、3G Cellular 接口**只能用于轮询 DCC**。

③ ISDN PRI 接口和 ISDN BRI 接口**既可以用于共享 DCC，也可以用于轮询 DCC**。但通过 ISDN BRI 接口实现 ISDN 专线时，**只能使用轮询 DCC**。

在 DCC 配置前应做好以下几个方面的准备。

（1）确定 DCC 应用的拓扑结构

① 哪些路由器将要提供 DCC 功能，这些提供 DCC 功能的路由器之间连接关系如何。

② 路由器的哪些接口提供 DCC 功能，提供 DCC 功能的接口发挥什么作用。

③ 采用何种传输介质，比如是通过 ISDN 网络还是 IP 网络等。

（2）确定 DCC 配置需要的数据

① 确定使用的接口类型并配置接口基本物理参数，具体参见本书第 3 章相关内容。

② 确定拨号接口使用的链路层封装模式（如 PPP、Frame Relay 等）。

③ 确定拨号接口支持的路由协议（如 RIP、OSPF 等）。

④ 确定拨号接口使用的网络层协议（如 IP 等）。

⑤ 确定 DCC 配置方法（轮询 DCC 或共享 DCC）。

（3）DCC 功能本身的参数配置

根据选定的 DCC 配置方法逐步配置基本 DCC 功能参数（轮询 DCC 或共享 DCC），实现 DCC 拨号功能。如果有特殊应用需求，还可增加配置 MP 捆绑、自动拨号、拨号串循环备份功能，也可以根据拨号链路的实际情况适当调整 DCC 拨号接口的属性参数。

4.3　配置轮询 DCC

轮询 DCC 适用于需要拨号的物理链路较多，连接情况较复杂的大中型站点。支持轮询 DCC 配置的 WAN 接口包括 ISDN PRI 接口、ISDN BRI 接口、Async 接口、3G Cellular 接口（**需要事先配置好这些 WAN 物理接口**，3G Cellular 接口的轮询 DCC 配置方法在本书第 3 章 3.8.2 小节和 3.8.3 小节有详细介绍），不能是 ADSL、VDSL、G.SHDSL 接口。

轮询 DCC 所包括的主要配置任务如下（**必需的只有前面三项**）。

① 配置拨号接口链路层协议和 IP 地址。

② 使能轮询 DCC 并配置 DCC 拨号 ACL 及与接口的关联。

③ 配置发起或接收轮询 DCC 呼叫。

④（可选）配置 DCC 拨号接口属性。

⑤（可选）配置 DCC 呼叫 MP 捆绑。

⑥（可选）配置拨号串循环备份。

⑦（可选）配置通过 DCC 实现动态路由备份。

下面各节依次介绍这些配置任务的具体配置方法。

4.3.1　配置拨号接口链路层协议和 IP 地址

在轮询 DCC 中，拨号接口的链路层协议和 IP 地址必须在 Dialer 接口视图下配置。 在 Dialer 接口的链路层可以封装的链路层协议包括 PPP 和 FR，还可在 Dialer 接口上配置 IP 地址（因为 ISDN PRI 接口、ISDN BRI 接口、Async 接口、3G Cellular 接口均支持 IP 协议，以提供路由功能）。具体的配置步骤如表 4-2 所示。

说明　当拨号接口的链路层协议为 PPP 时，还可以配置 PAP 或者 CHAP 验证，具体将在本章后面介绍 PPP 协议配置时介绍。

表 4-2　Dialer 接口链路层协议和 IP 地址的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface dialer** *interface-number* 例如：[Huawei] **interface dialer 0**	创建并进入 Dialer 接口视图。参数 *interface-number* 用来指定 Dialer 接口的编号，取值范围是 AR150/150-S/200/200-S 系列、AR1200/1200-S 系列、AR2201-48FE/2201-48FE、AR2202-48FE 和 AR2204/2204-S 为 0～127 的整数；AR2220L、AR2220/2200-S 和 AR2240 为 0～511 的整数；AR3200 系列为 0～1 023 的整数；对于 AR2240-S，不同的主控板取值不同：SRU40 和 SRU60 为 0～511 的整数，SRU80 为 1 024
3	**link-protocol** [**ppp** | **fr**] 例如：[Huawei-Dialer0] **link-protocol ppp**	配置拨号接口的链路层协议为 PPP 或者 FR（帧中继） 缺省情况下，除以太网接口外，其他接口封装的链路层协议均为 PPP。当封装 FR 协议时，缺省情况下，帧的封装格式为 IETF

（续表）

步骤	命令	说明
3	**link-protocol** [**ppp** | **fr**] 例如：[Huawei-Dialer0] **link-protocol ppp**	【注意】通过 Async 接口或 3G Cellular 接口进行 DCC 拨号时，物理接口及所属的 Dialer 接口封装的链路层协议都不能为 FR
4	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-Dialer0]**ip address 129.102.0.1 255.255.255.0**	（二选一）配置 Dialer 接口的 IP 地址 本命令已在第 3 章 3.15.1 小节表 3-38 中做了详细介绍，参见即可
	ip address ppp-negotiate 例如：[Huawei-Dialer0]**ip address ppp-negotiate**	（二选一）配置本端接口接受 PPP 协商产生的由对端分配的 IP 地址 本命令已在第 3 章 3.15.1 小节表 3-38 中做了详细介绍，参见即可

4.3.2 使能轮询 DCC 并配置 DCC 拨号 ACL 及与接口的关联

要配置轮询 DCC，首先要在物理拨号接口，或者逻辑 Dialer 接口上使能轮询 DCC 功能。**在物理接口上直接使能轮询 DCC 仅适用于单个接口向一个或多个对端发起呼叫的情况；在 Dialer 接口上使能轮询 DCC 可适用于多个接口向单个或多个对端发起呼叫，**当然也可用于单个接口向外发起呼叫。

然后还需要配置用于控制通过拨号线路发送报文的 ACL。要想使 DCC 正常发送报文，必须配置 DCC 拨号控制列表，并将对应拨号接口（如物理接口、Dialer 接口）通过 **dialer-group** 命令与拨号控制列表关联起来，如果缺少此项配置则 DCC 无法正常发送报文。DCC 拨号控制列表既可以直接配置数据报文的过滤条件，也可以引入访问控制列表中的过滤规则。

根据报文是否符合拨号 ACL 的允许（permit）或拒绝（deny）条件，DCC 的控制原则如下。

① 符合拨号 ACL permit 条件的报文，或者不符合拨号 ACL deny 条件的报文，如果相应链路已经建立，DCC 将通过该链路发出报文，并清零 Idle 超时定时器；如果链路没有建立则发出新呼叫。

② 不符合拨号 ACL permit 条件的报文，或者符合拨号 ACL deny 条件的报文，如果相应的链路已经建立，DCC 将通过此链路发出报文，但不清零 Idle 超时定时器；如果相应链路没有建立，则不发出呼叫并丢弃此报文。

使能轮询 DCC 功能和配置 DCC 拨号 ACL 的具体步骤如表 4-3 所示（**仅以在 Dialer 接口上配置为例进行介绍**）。

表 4-3　　使能轮询 DCC 并配置 DCC 拨号 ACL 及与接口关联的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dialer-rule** 例如：[Huawei] **dialer-rule**	进入 Dialer-rule 视图

（续表）

步骤	命令	说明
3	**dialer-rule** *dialer-rule-number* { **acl** { *acl-number* | **name** *acl-name* } | **ip** { **deny** | **permit** } | **ipv6** { **deny** | **permit** } } 例如：[Huawei-dialer-rule] **dialer-rule 1 ip permit**	配置某个拨号访问组对应的拨号访问控制列表，指定引发 DCC 呼叫的条件。命令中的参数和选项说明如下 ● *dialer-rule-number*：指定拨号访问组的编号，取值范围为 1～255 的整数。取值要与下面 **dialer-group** 命令中的 *group-number* 参数值一致 ● **acl** { *acl-number* | **name** *acl-name* }：多选一选项，指定配置的拨号访问控制列表过滤报文时需要满足的 ACL 编号或 ACL 名称 ● **ip** { **deny** | **permit** }：多选一选项，指定配置的拨号访问控制列表禁止或允许 IPv4 协议的数据报文 ● **ipv6** { **deny** | **permit** }：多选一选项，指定配置的拨号访问控制列表禁止或允许 IPv6 协议的数据报文 缺省情况下，未配置任何拨号访问控制列表，可用 **undo dialer-rule** *dialer-rule-number* [**acl** | **ip** | **ipv6**] 取消对应拨号访问组的拨号访问控制设置
4	**quit** 例如：[Huawei-dialer-rule] **quit**	退出 Dialer-rule 视图，返回系统视图
5	**interface** *interface-type interface-number* 例如：[Huawei] **interface interface** serial 1/0/0:15 或 **interface dialer** *interface-number* 例如：[Huawei] **interface dialer 0**	进入物理拨号接口（**单个接口向一个或多个对端发起呼叫时**）或者 Dialer 接口（**单个，或者多个接口向单个或多个对端发起呼叫时**）视图
6	**dialer enable-circular** 例如：[Huawei-Serial1/0/0:15] **dialer enable-circular** 或 例如：[Huawei-Dialer0] **dialer enable-circular**	在拨号接口上使能轮询 DCC 功能 缺省情况下，接口上去使能轮询 DCC 功能，可用 **undo dialer enable-circular** 命令去使能轮询 DCC 功能
7	**dialer-group** *group-number* 例如：[Huawei-Serial1/0/0:15] **dialer-group** 1 或 例如：[Huawei-Dialer0] **dialer-group** 1	配置拨号接口的拨号访问组。参数 *group-number* 用来指定接口所属的拨号访问组的编号，这个拨号访问组由第 3 步的 **dialer-rule** 命令设定，要与其中的 *dialer-rule-number* 参数值一致，取值范围为 1～255 的整数 缺省情况下，未配置 DCC 拨号控制列表及拨号接口所属的拨号访问组，可用 **undo dialer-group** 命令将接口从此拨号访问组中删除 【注意】配置此命令前，请先使用第 3 步中的 **dialer-rule** 命令配置 DCC 拨号控制列表，且一个接口只能属于一个 **dialer-group**，若重复配置，则将覆盖原来的配置

4.3.3 配置发起或接收轮询 DCC 呼叫

要在路由器上配置轮询 DCC 功能，必须配置该路由器设备能够发起或接收轮询 DCC 呼叫。通过前面 4.2.2 小节的学习已经知道，当使用轮询 DCC 方法来配置按需拨号时，可以有两种方法配置 DCC 参数。

① 在物理接口上直接配置 DCC 参数：**适用于单个接口向一个（或多个）对端发起呼叫。**

② 在 Dialer 接口上配置 DCC 参数：**适用于多个接口向单个（或多个）对端发起呼叫**，也可用于单个接口向外发起呼叫。

当采用在 Dialer 接口上配置 DCC 参数的方法时，拨号循环组将一个 Dialer 接口与一组物理拨号接口对应起来，对这个 Dialer 接口的 DCC 呼叫配置将会自动地被该拨号循环组中的所有物理接口继承。配置完拨号循环组相关参数后，如果逻辑 Dialer 接口对应多个目的地，拨号循环组中的任一物理接口都可以呼叫设定好的任意一个目的地。

根据网络拓扑结构及 DCC 拨号需求的不同，如一个接口既发出呼叫又接收呼叫、多个接口既发出呼叫又接收呼叫等情况，可以灵活组合使用以下介绍的轮询 DCC 配置中的一种或几种。

说明 应用轮询 DCC 方法配置按需拨号时，拨号双方可选配置 PAP 或 CHAP 认证，但是如果一方配置认证则另一方也必须配置。在具体组网应用中，出于确保拨号身份的安全性，推荐配置认证，但同时注意以下约束。

在发送端，如果在物理接口直接使能 DCC，则直接在物理接口上配置 PAP 或 CHAP 认证；如果通过拨号循环组使能 DCC，则在 Dialer 接口上配置 PAP 或 CHAP 认证。

在接收端配置 PAP 或 CHAP 认证时，建议在物理接口和 Dialer 接口上都配置。因为当物理接口接收到 DCC 呼叫请求时，首先进行 PPP 协商并认证拨入用户的合法性，然后将呼叫转交给上层 DCC 模块进行处理。

1. 发起呼叫的几种情况下的配置

（1）一个接口向一个对端发起呼叫

在一个接口向一个对端发起呼叫的情况下，DCC 呼叫配置**既可以在物理拨号接口上配置，也可以在 Dialer 接口上配置。**

如图 4-8 所示，本端单接口 interface1/0/0（简写为 if1/0/0）向对端单接口 if1/0/0 发起 DCC 呼叫。向单个对端发起呼叫时，可使用 **dialer number** 命令或 **dialer route** 命令配置拨号串。由于是从本端单个接口发起呼叫，因此可选择使用拨号循环组配置 DCC。可选配置 PAP 或 CHAP 认证。具体配置步骤如表 4-4 所示（不包括 PPP 认证）。

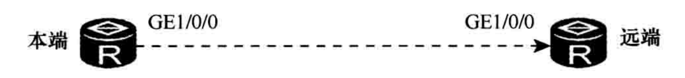


图 4-8 一个接口向一个对端发起呼叫的示意图

表 4-4 一个接口向一个对端发起呼叫时的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial 1/0/0:15** 或 例如：**interface dialer** *interface-number* 例如：[Huawei] **interface dialer 0**	进入物理接口（**适用于单个接口向一个（或多个）对端发起呼叫**）或 Dialer 接口（**主要适用于多个接口向单个（或多个）对端发起呼叫**）视图 单接口向对端发起呼叫时可以在物理接口上配置，也可以在 Dialer 接口上配置

（续表）

步骤	命令	说明
3	**dialer number** *dial-number* [**autodial**] 例如：[Huawei-Serial1/0/0:15] **dialer number** 12345 或 例如：[Huawei-Dialer0] **dialer number** 12345	（三选一）在物理接口或者在 Dialer 接口上配置呼叫一个对端的拨号串（通常就是对端的电话号码）。命令中的参数和选项说明如下 ● *dial-number*：指定以上接口下呼叫一个对端的拨号串，为 1～30 个字符，支持空格，**但区分大小写** ● **autodial**：可选项，配置接口根据拨号串自动拨号。缺省情况下，未使能自动拨号 autodial 功能 【注意】如果拨号接口的 IP 地址配置为接受 PPP 协商产生的由对端分配的 IP 地址，则需要使用本命令来指定拨号串，不能使用下面的 **dialer route ip** 命令。使用轮询 DCC，主叫端和被叫端的拨号串配置都允许重复 设备支持在同一个拨号接口下多次执行本命令配置呼叫一个对端的多个拨号串，但如果选择 **autodial** 可选项，那么该拨号接口只能执行一次 **dialer number** 命令配置，呼叫一个对端的拨号串 缺省情况下，没有设定去往对端的拨号串，可用 **undo dialer number** *dial-number* 命令删除已设定的拨号串
	dialer route ip *next-hop-address* [**user** *hostname* | **broadcast**] * *dial-string* [**autodial** | **interface** *interface-type interface-number*]* 例如：[Huawei-Dialer0]**dialer route ip** 10.10.10.5 **user** winda 123456	（三选一）在 **Dialer 接口**上配置从一个拨号接口呼叫一个指定目的地址（**即拨号路由**）。命令中的参数和选项说明如下 ● *next-hop-address*：指定拨号目的地的 IP 地址，且该 IP 地址为直连的下一跳地址 ● **user** *hostname*：可多选参数，指定对端用户名，用于对端接受本端呼叫时所进行的用户认证。若配置该参数，则必须配置 PPP 认证 ● **broadcast**：可多选选项，设置广播报文（比如，OSPF、RIP 报文）可以从这条链路发送 ● *dial-string*：指定去往对端的拨号串（也是拨号时所用的对端电话），为 1～30 个字符，支持空格，**但区分大小写** ● **autodial**：可多选选项，配置接口根据拨号串自动拨号。选择此可选项时，路由器会每隔一定时间自动尝试用本 **dialer route** 拨号，该时间的间隔由 **dialer timer autodial** 命令设置。缺省情况下，未使能自动拨号 autodial 功能 ● **interface** *interface-type interface-number*：可选参数，指定拨号时所用的物理拨号接口 【注意】当接口的链路层协议为 FR 时，不能配置该命令，只能使用 **dialer number** 命令配置拨号串 当拨号接口为 3G Cellular 接口或 Dialer 接口中包含的物理接口为 3G Cellular 时，不能配置该命令，只能使用 **dialer number** 命令配置拨号串 一个拨号接口（包括物理接口和 Dialer 接口）可以配置多条 **dialer route**。一个目的地址也可配置多条 **dialer route**，到同一目的的 **dialer route** 间实现相互备份。但一条 **dialer** route 命令只能对应一个目的地址，需要从一个 dialer 接口呼叫多个目的地址时，需要重复执行本命令 缺省情况下，系统没有定义拨号路由，可用 **undo dialer route ip** *next-hop-address* [**user** *hostname*] [*dial-string*] [**interface** *interface-type interface-number*]命令删除指定的一条拨号路由

（续表）

步骤	命令	说明
3	**dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**] 例如：[Huawei-Serial1/0/0:15] **dialer route ip 10.10.10.5 user** winda 123456	（三选一）在**物理拨号接口**上配置从一个拨号接口呼叫一个指定目的地址。命令中的参数和选项，及其他说明同上一步介绍，参见即可。不同的只是在物理接口上配置时不能再配置 **interface** *interface-type interface-number* 可选参数 缺省情况下，系统没有定义拨号路由，可用 **undo dialer route ip** *next-hop-address* [**user** *hostname*] [*dial-string*]命令删除指定的一条拨号路由

（2）一个接口向多个对端发起呼叫

在一个接口向多个对端发起呼叫的情况下，与前面介绍的一个接口向一个对端发起呼叫一样，DCC 呼叫配置**既可以在物理拨号接口上配置，也可以在 Dialer 接口上配置**。

如图 4-9 所示，本端单接口 GE1/0/0 向多个对端接口 GE1/0/0、GE2/0/0、GE2/0/1 等发起 DCC 呼叫。由于需要向多个对端发起呼叫，因此**必须使用 dialer route** 命令配置拨号串和目的地址（不能使用 **dialer number** 命令配置）。同样由于是从本端单个接口发起呼叫，因此可选择使用拨号循环组配置 DCC。可选配置 PAP 或 CHAP 认证。

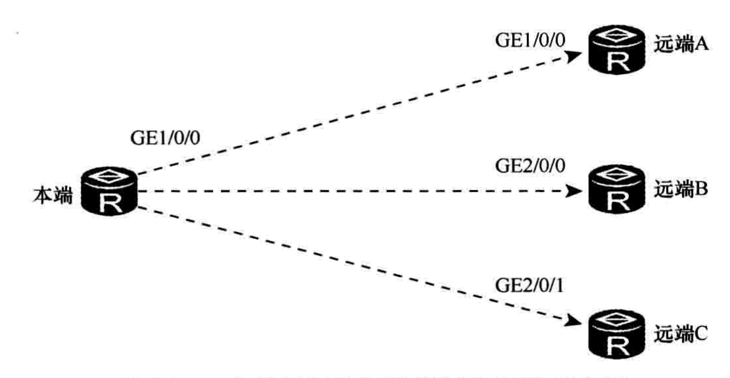


图 4-9　一个接口向多个对端发起呼叫的示意图

一个接口向多个对端发起呼叫的配置步骤与前面介绍的一个接口向一个对端发起呼叫时的配置步骤基本一样，只是不能使用表 4-4 中的 **dialer number** 命令来指定拨号串（其他完全一样），必须使用 **dialer route** 命令来指定到达多个目的地址的拨号串（多个目的地址的拨号串必须通过多条 **dialer route** 命令来配置），但也既可在物理拨号接口上配置，又可在 Dialer 接口上配置。其他方面参见表 4-4 中的各步说明。

（3）多个接口向多个对端发起呼叫

在多个接口向多个对端发起呼叫的情况下，DCC 配置**必须在 Dialer 接口上配置**。

如图 4-10 所示，本端多接口 GE1/0/0、GE1/0/1 和 GE2/0/0 向多个对端接口 GE1/0/0、GE2/0/0、GE2/0/1 发起 DCC 呼叫。由于向多个对端发起呼叫，因此必须使用 **dialer route** 命令配置拨号串和多个目的地址；由于是从多个接口发起呼叫，因此**必须使用拨号循环组配置 DCC**。可选配置 PAP 或 CHAP 认证。具体配置步骤如表 4-5 所示（不包括 PPP 认证）。

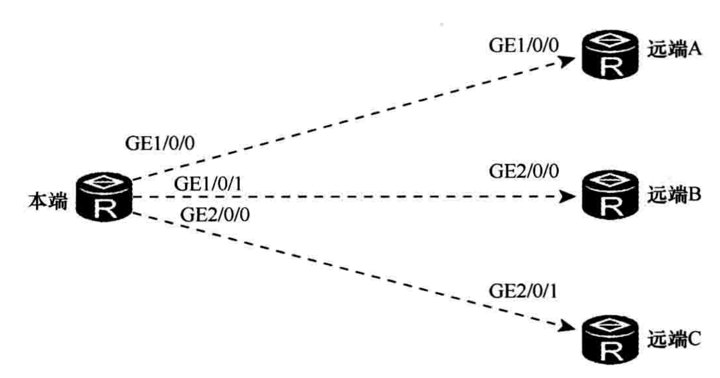


图 4-10　多个接口向多个对端发起呼叫的示意图

表 4-5　　多个接口向多个对端发起呼叫的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface dialer** *interface-number* 例如：[Huawei] **interface dialer 0**	进入 Dialer 接口视图
3	**dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * *dial-string* [**autodial** | **interface** *interface-type interface-number*] * 例如：[Huawei-Dialer0] **dialer route ip** 10.10.10.5 **user** winda 123456	在 **Dialer 接口**上配置从一个拨号接口呼叫一个或多个指定目的地址（**即拨号路由**）。其他参见表 4-4 中第 3 步介绍 需要配置多条这个命令来为多个目的地址配置拨号路由
4	**quit** 例如：[Huawei-Dialer0] **quit**	退出 Dialer 接口视图，返回系统视图
5	**interface** *interface-type interface-number* 例如：[Huawei]**interface serial** 1/0/1:15	键入要与同一个拨号循环组（Dialer Circular Group）绑定的物理拨号接口，进入接口视图
6	**dialer circular-group** *number* 例如：[Huawei-Serial1/0/1:15] **dialer circular-group** 0	将物理接口加入指定的拨号循环组中。参数 *number* 应该与 **interface dialer** *interface-number* 命令中的 *interface-number* 保持一致。执行该命令后，接口上会自动使能轮询 DCC 功能 缺省情况下，物理接口不属于任一个拨号循环组，可用 **undo dialer circular-group** 命令取消配置物理接口所属的拨号循环组
7	**dialer priority** *priority* 例如：[Huawei-Serial1/0/0:15] **dialer priority** 5	配置物理接口在拨号循环组中的优先级，取值范围为 1～127 的整数。数值越大优先级越高，缺省的优先级为 1 【说明】在拨号过程中，拨号循环组中的物理接口不使用自己的 IP 地址，而是继承 Dialer 接口的 IP 地址。在同一视图下多次执行本命令，新的配置覆盖老的配置 缺省未创建任何 Dialer 接口，物理接口也不属于任何拨号循环组，物理接口加入拨号循环组时缺省优先级为 1，可用 **undo dialer priority** 命令恢复优先级为缺省值
8	重复步骤 5～8，为其他物理拨号接口配置所绑定的拨号循环组	

2. 接收呼叫的几种情况下的配置

（1）一个接口从一个对端接收呼叫

一个接口从一个对端接收呼叫的情形参见图 4-8，不同的只是此时是从对端向本端呼叫（**箭头方向相反**）。即本端单接口 GE1/0/0 从对端单接口 GE1/0/0 接收 DCC 呼叫。由于本端为单个接口，所以既可以在对应物理拨号接口上配置 DCC，又可以选择使用拨号循环组（在 Dialer 接口上）来配置 DCC。可选配置 PAP 或 CHAP 认证。

缺省情况下，本端一个接口接收一个对端呼叫时**本端可不用做任何额外配置**，只需要配置好用于对端呼叫时所需的用户账户、对端拨号时指定拨号串的线路即可。只是在当需要对对端（主叫方）的 *next-hop-address*、*hostname* 进行验证时，或者指定的本端物理接口既需要发起呼叫又需要接收呼叫时，才需要按照表 4-4 中除 **dialer number** 命令外的其他步骤进行配置。

（2）一个接口从多个对端接收呼叫

一个接口从多个对端接收呼叫的情形参见图 4-9，只不过此时是从多个对端向一个本端接口发起呼叫（**箭头方向相反**）。即本端单接口 GE1/0/0 从多个对端接口 GE1/0/0、GE2/0/0、GE2/0/1 接收 DCC 呼叫。由于本端为单个接口，因此既可在物理拨号接口上配置，也可以选使用拨号循环组（在 Dialer 接口上）配置 DCC。可选配置 PAP 或 CHAP 认证。

同样，缺省情况下，本端一个接口接收多个对端呼叫时**本端也可不用做任何额外配置**，只需要配置好用于对端呼叫时所需的用户账户、对端拨号时指定的拨号串的线路即可。只是在当需要对对端（主叫方）的 *next-hop-address*、*hostname* 进行验证时，或者指定的本端物理接口既需要发起呼叫又需要接收呼叫时，才需要按照表 4-4 中除 **dialer number** 命令外的其他步骤进行配置。

（3）多个接口从多个对端接收呼叫

多个接口从多个对端接收呼叫的情形参见图 4-10，只不过此时是从多个对端向多个本端接口发起呼叫（**箭头方向相反**）。即本端多接口 GE1/0/0、GE1/0/1 和 GE2/0/0 从多个对端接口 GE1/0/0、GE2/0/0 等接收 DCC 呼叫。由于本端为多个接口，因此**必须使用拨号循环组（在 Dialer 接口上）配置 DCC**。可选配置 PAP 或 CHAP 认证。

具体的配置步骤仍可按照表 4-5 所示步骤进行，但第 3 步在当需要对对端（主叫方）的 *next-hop-address*、*hostname* 进行验证时，或者指定的本端物理接口既需要发起呼叫又需要接收呼叫时才需要配置。

4.3.4 配置 DCC 拨号接口属性

拨号接口（包括物理拨号接口和 Dialer 接口）一旦创建，就会赋予一系列属性参数的缺省值，因此本项配置任务为可选项，可以根据实际需要进行修改。具体主要包括以下几个方面。

（1）链路空闲时间

如果某个拨号接口发出呼叫，则可以设置当链路空闲超过了指定时间后，DCC 将断开链路。这个空闲时间也即链路中不存在符合拨号访问控制列表的 permit 条件的报文传送时间。

（2）下次呼叫发起前的链路断开时间

当 DCC 呼叫链路因故障或挂断等原因进入断开状态时，必须经过指定时间后才能建立新的拨号连接（即进行下一次呼叫的间隔时间），从而避免对端 PBX 设备过载。

（3）接口竞争时的链路空闲时间

当 DCC 开始发起新呼叫时，如果所有通道都被占满则进入“竞争”状态。通常一条链路建立后 Idle 超时定时器将起作用。但如果同时去往另一目的地址的呼叫发生，则会引起竞争，此时 DCC 使用 Compete-idle 超时定时器取代 Idle 超时定时器，即链路空闲时间达到 Compete-idle 超时定时器的规定后将自动断开。

（4）呼叫建立超时的时间

为了有效控制发起呼叫到呼叫连接建立之间允许等待的时间，可以配置 Wait-carrier 定时器，可规定如果在指定时间内呼叫仍未建立则 DCC 将终止该呼叫。

（5）拨号接口缓冲队列长度

没有为拨号接口配置缓冲队列的情况下，当拨号接口收到一个报文时，如果此时连接还没有成功建立，则这个报文将会被丢弃。如果为拨号接口配置了缓冲队列，则在连接成功建立之前报文将被缓存而不是被丢弃，待连接成功后再发送。

（6）自动拨号时间间隔

启动自动拨号功能后，路由器启动后，DCC 将自动尝试拨号连接对端，无需通过数据报文进行触发。如果无法与对端正常建立拨号连接，则每隔一段时间 DCC 会再次自动尝试建立拨号连接。与数据触发的非自动拨号 DCC 相比，该连接建立后不会因超时而自动挂断（即 **dialer timer idle** 命令对自动拨号不起作用）。

以上拨号接口属性的具体配置步骤如表 4-6 所示（**各属性参数配置没有严格的先后次序**）。

说明　本节所说的“拨号接口”既可以是物理拨号接口，也可以是 Dialer 接口，具体在哪里配置要根据上节介绍的对应情形而定，即单接口发起拨号呼叫时既可以在物理接口上配置，也可以在 Dialer 接口上配置，而多接口发起拨号呼叫时一定要在 Dialer 接口上配置。

表 4-6　DCC 拨号接口属性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface serial** 1/0/0:15 或 **interface dialer** *interface-number* 例如：[Huawei] **interface dialer** 0	进入物理接口（**适用于单个接口向一个（或多个）对端发起呼叫**）或 Dialer 接口（**主要适用于多个接口向单个（或多个）对端发起呼叫**）视图 单接口向对端发起呼叫时可以在物理接口上配置，也可以在 Dialer 接口上配置

（续表）

步骤	命令	说明
3	**dialer timer idle** *seconds* 例如：[Huawei-Serial1/0/1:15] **dialer timer idle** 100 或 例如：[Huawei-Dialer0] **dialer timer idle** 100	配置拨号接口允许链路空闲时间，取值范围为 0～65 535 s，取整数 【说明】为了避免链路建立以后，因长时间没有数据传输而导致的资源和金钱上的浪费，可以通过该命令配置允许链路空闲的时间。当链路上没有数据传输的时间达到本命令设置的时间时，链路自动断开 在同一视图下多次执行本命令，新的配置覆盖老的配置。本命令不影响已经建立的呼叫，对后续建立的呼叫有影响 缺省情况下，允许链路空闲的时间为 120 s，可用 **undo dialer timer idle** 命令恢复缺省情况
4	**dialer timer enable** *seconds* 例如：[Huawei-Serial1/0/1:15] **dialer timer enable** 10 或 例如：[Huawei-Dialer0] **dialer timer enable** 10	配置拨号接口下次呼叫发起前的链路断开时间，取值范围为 5～65 535 s，取整数 【说明】当 DCC 呼叫链路因故障或挂断等原因导致进入断开状态后，该链路必须经过指定时间后才能建立新的拨号连接（即进行下一次呼叫的间隔时间），从而避免对对端 PBX 设备过载 缺省情况下，下次呼叫发起前的间隔时间为 5 s，可用 **undo timer enable** 命令恢复下次呼叫发起前的间隔时间为缺省值
5	**dialer timer compete** *seconds* 例如：[Huawei-Serial1/0/1:15] **dialer timer compete** 5 或 例如：[Huawei-Dialer0] **dialer timer compete** 5	配置当拨号接口发生呼叫竞争后的接口空闲时间，取值范围为 0～65 535 s，取整数 【说明】所谓竞争，是指当 DCC 开始一个呼叫时没有空闲的通道可以使用的状态。通常情况下，当一条链路建立后，**dialer timer idle** 定时起作用。但若此时有一个去往另一个目的地址的呼叫发生，引起了竞争，则 DCC 使用 **dialer timer compete** 定时取代 **dialer timer idle** 定时，即链路空闲时间达到 **dialer timer compete** 超时定时器的规定后将自动断开 本命令配置的竞争空闲时间要小于第 3 步中的 **dialer timer idle** 命令配置的链路空闲时间 缺省情况下，接口发生呼叫竞争后的空闲时间为 20 s，可用 **undo dialer timer compete** 命令恢复发生呼叫竞争后的接口空闲时间为缺省情况
6	**dialer timer wait-carrier** *seconds* 例如：[Huawei-Serial1/0/1:15] **dialer timer wait-carrier** 20 或 例如：[Huawei-Dialer0] **dialer timer wait-carrier** 20	配置拨号接口呼叫建立超时间隔，取值范围为 0～65 535 s，取整数 【说明】为了有效控制发起呼叫到呼叫连接建立之间允许等待的时间，用户可以使用此命令配置呼叫建立超时时间。配置此命令后，若在指定时间内呼叫未建立，则 DCC 将终止该呼叫 在同一视图下多次配置该命令，新的配置覆盖老的配置 缺省情况下，呼叫建立超时时间为 60 s，可用 **undo dialer timer wait-carrier** 命令恢复为缺省情况

（续表）

步骤	命令	说明
7	**dialer queue-length** *packets* 例如：[Huawei-Serial1/0/1:15] **dialer queue-length** 10 或 例如：[Huawei-Serial1/0/0:15] **dialer queue-length** 10	配置拨号接口缓冲队列长度，取值范围是1～100的整数 【说明】在没有为拨号接口配置缓冲队列的情况下，当拨号接口收到一个报文时，如果此时连接还没有成功建立，则这个报文将被丢弃。如果为拨号接口配置了缓冲队列，则在连接成功建立之前报文将被缓存，待连接成功后再发送 在同一视图下多次执行本命令，新的配置覆盖老的配置。另外，如果接口的缓冲队列长度设置较长，则该接口丢包率相应较小，但占用系统的资源也较多。配置时建议该值不要大于20 缺省情况下，没有配置拨号接口缓冲队列，可用 **undo dialer queue-length** 命令恢复为缺省情况
8	**dialer timer autodial** *seconds* 例如：[Huawei-Serial1/0/1:15] **dialer timer autodial** 30 或 例如：[Huawei-Serial1/0/0:15] **dialer timer autodial** 30	配置DCC自动拨号的时间间隔，即指定发起下次呼叫尝试的间隔时间，取值范围为1～604 800 s，取整数 【说明】该功能只能和轮询DCC结合使用。自动拨号是指：在路由器启动后，DCC将自动尝试拨号连接对端，无需通过数据报文进行触发。若无法与对端正常建立拨号连接，则每隔一段时间DCC将再次自动尝试建立拨号连接 缺省情况下，未配置自动拨号功能。当启动自动拨号功能后，自动拨号间隔缺省为300 s。使用 **dialer route** 命令配置拨号串时，通过指定 **autodial** 参数来启动自动拨号功能，可用 **undo dialer timer autodial** 命令恢复为缺省情况

4.3.5 配置DCC呼叫MP捆绑

有时为了满足用户的数据传输速率需求，可以捆绑配置一次DCC呼叫使用多个PPP连接，即多条PPP链路绑定成一条MP链路。以CE1/PRI接口为例，一个PPP连接的速率是64 kbit/s，如果用户需要1 024 kbit/s的速率，就可以配置MP最大捆绑链路数为16。具体配置步骤如表4-7所示（仅可在Dialer接口下配置）。

表4-7　　DCC呼叫MP捆绑的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface dialer** *interface-number* 例如：[Huawei] **interface dialer** 0	进入要捆绑PPP链路的Dialer接口视图
3	**link-protocol ppp** 例如：[Huawei-Dialer0] **link-protocol ppp**	（可选）配置拨号接口的链路层协议为PPP 缺省情况下，除以太网接口外，其他接口封装的链路层协议均为PPP
4	**ppp mp** 例如：[Huawei-Dialer0] **ppp mp**	配置封装PPP协议的接口工作在MP方式 这是按照PPP链路用户名查找VT实现MP的方式，根据验证通过的对端用户名查找对应的虚拟接口模板，相同用户名绑定到一个虚拟接口模板实现MP **配置本命令的同时，必须在接口下配置PPP双向认证** 缺省情况下，封装PPP的接口工作在普通PPP方式下，可用 **undo ppp mp** 命令恢复为缺省的PPP方式

（续表）

步骤	命令	说明
5	**ppp mp max-bind** *max-bind-number* 例如：[Huawei-Dialer0] **ppp mp max-bind** 10	（可选）配置 MP 最大捆绑链路数，取值范围为 1～32 的整数 缺省情况下，MP 最大捆绑链路数的值为 16，可用 **undo ppp mp max-bind** 命令恢复为缺省值 【注意】设备最多支持 32 成员接口加入 MP。MP 下可以进行数据传送的链路数达到最大捆绑链路数后，不允许新的可用的 PPP 链路加入。如果超过 32 个成员接口加入 MP，则在 LCP 协商后无法成功绑定 MP 的成员接口就会 Down，之后再次进行 LCP 协商尝试绑定 MP，如此未绑定成功的成员接口便会反复的 Up 和 Down

4.3.6 配置拨号串循环备份

在轮询 DCC 中，可以配置多个呼叫**同一个对端**的目的地址及拨号串，以用于拨号串的循环备份。如果是单接口呼叫，则既可以在物理拨号接口上配置，也可以在 Dialer 接口上配置；如果是多接口呼叫，则必须在 Dialer 接口上配置。

拨号串循环备份的配置的方法就是使用表 4-4 第 3 步中的 **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial** | **interface** *interface-type interface-number*] *命令（在 Dialer 接口上配置时），或者 **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**]命令（在物理拨号接口上配置时），为呼叫**同一对端**配置多条带有不同目的地址（*next-hop-address*）、不同拨号串（*dial-string*）（当然这要在对端提供了多个可用的目的地址和拨号串时才能进行配置）的以上命令。命令中的具体参数和选项说明参见 4.3.3 小节表 4-4 中的第 3 步。

4.3.7 配置通过 DCC 实现动态路由备份

动态路由备份很好地集成了备份和路由功能，提供了可靠的连接和规范的按需拨号服务。动态路由备份的特点如下。

① 动态路由备份主要是针对动态路由协议产生的路由进行备份，也可以对静态路由和直连路由进行备份。

② 动态路由备份不对特定接口或特定链路进行备份，适用于多接口和多路由器的情况。

③ 动态路由备份的主链路断开时备份链路将自动启动，不会导致拨号延迟（该延迟未包括路由收敛时间）。

④ 动态路由备份不依赖于具体的路由协议，但可以和 RIP-1、RIP-2、OSPF、IS-IS、BGP 等路由协议配合工作。

注意 有些路由协议（如 BGP）默认使用优选路由，若到达被监控网段的主链路故障中断，启用备份链路之后，备份链路通过 BGP 协议学习到达被监控网段的路由；当主链路再次启用后，主链路通过 BGP 协议学到的路由和备份链路学到的路由相比可能不是最优路由，因此继续使用从备份链路学到的路由，导致动态路由监控失败，备份链路在主链

路恢复时无法挂断。需要使用下面的方法来解决这种问题：①备份链路的 IP 地址要大于主链路的 IP 地址；②配置负载分担，即让同一路由可以通过多条链路学到。

配置动态路由备份后，自动拨号失效。动态路由备份的具体配置步骤如表 4-8 所示。同样，要根据不同的呼叫情形，选择在物理拨号接口上配置，或者在 Dialer 接口上配置。

表 4-8　　DCC 动态路由备份的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**standby routing-rule** *group-number* **ip** *ip-address* { *mask* | *mask-length* } 例如：[Huawei] **standby routing-rule** 1 **ip** 20.0.0.1 255.0.0.0	创建动态路由备份组，并将被监控网段加入动态路由备份组。这样当到所有被监控网段都无有效路由时，则拨号启用备用链路。命令中的参数说明如下 ● *group-number*：指定创建的动态路由备份组编号，取值范围为 1～255 的整数 ● *ip-address*：指定需监控的网段地址 ● *mask* | *mask-length*：指定需监控的网段地址的子网掩码（选择 *mask* 二选一参数时）或子网掩码长度（选择 *mask-length* 二选一参数时） 【说明】使用相同的 *group-number* 参数重复执行本命令时，可以配置一个路由备份组监控不同的网段，各监控网段之间为“或”的关系，即**当到达备份组中指定的所有网段都不存在有效路由时，设备才拨通备份链路** 缺省情况下，没有创建动态路由备份组，可用 **undo standby routing-rule** *group-number* [**ip** *ip-address* { *mask* | *mask-length* }] 命令删除动态路由备份组，或从动态路由备份组中删除被监控网段
3	**interface** *interface-type interface-number* 例如：[Huawei]**interface serial** 1/0/0:15 或 **interface dialer** *interface-number* 例如：[Huawei] **interface dialer** 0	进入配置动态路由备份的物理接口（**适用于单个接口向一个（或多个）对端发起呼叫**）或 Dialer 接口（**主要适用于多个接口向单个（或多个）对端发起呼叫**）视图 单接口向对端发起呼叫时的动态路由备份可以在物理接口上配置，也可以在 Dialer 接口上配置
4	**standby routing-group** *group-number* 例如：[Huawei-Serial1/0/1:15] **standby routing-group** 1 或 例如：[Huawei-Dialer0] **standby routing-group** 1	在以上拨号备份接口（可以是物理拨号接口，也可以是 Dialer 接口）上启用动态路由备份功能。参数 *group-number* 用来指定应用动态路由备份的备份组编号，取值范围为 1～255 的整数 【说明】通过创建动态路由备份组，将被监控网段加入动态路由备份组。当到被监控网段无有效路由时，则拨号启用备用链路。备用链路的选择需要根据本命令确定。例如：定义了动态路由备份组 1（监控到网段 20.0.0.0/8 的路由），且在接口 Serial1/0/0:15 上执行 **standby routing-group 1** 命令。当到网段 20.0.0.0/8 无可用路由时，则需要从接口 Serial1/0/0 拨起备用链路 在配置该命令前，请确保备份拨号接口上已经配置基本 DCC 功能，已经执行第 2 步中的 **standby routing-rule** 命令创建动态路由备份组 缺省情况下，禁用动态路由备份功能，可用 **undo standby routing-group** *group-number* 命令删除指定备份组的在本地拨号接口上的动态路由备份功能

（续表）

步骤	命令	说明
5	**standby timer routing-disable** *seconds* 例如：[Huawei-Serial1/0/1:15] **standby timer routing-disable** 20 或 例如：[Huawei-Dialer0] **standby timer routing-disable** 20	（可选）配置主链路重新接通后断开备份链路的延迟时间，取值范围为 0～65 535s，取整数，当取值为 0 时，当主链路接通以后，系统会立即断开备份链路 在主链路接通后，为了防止路由振荡，可以经过指定延迟时间再断开备份链路。缺省情况下，主链路接通后断开备份链路的延迟时间为 20 s，可用 **undo standby timer routing-disable** 命令恢复缺省情况
6	**quit** 例如：[Huawei-Serial1/0/1:15] **quit** 或 例如：[Huawei-Dialer0] **quit**	退出物理拨号接口或者 Dialer 接口视图，返回系统视图
7	**dialer timer warmup** *seconds* 例如：[Huawei-Serial1/0/1:15] **dialer timer warmup** 30 或 例如：[Huawei-Dialer0] **dialer timer warmup** 30	配置动态路由备份功能在系统启动后多久生效，在这段时间内不对备份链路进行呼叫，取值范围为 0～65 535s，取整数缺省情况下，动态路由备份功能在系统启动 30 s 后生效，可用 **undo dialer timer warmup** 命令恢复缺省情况 【说明】因为缺省情况下，系统启动后会进行配置恢复，配置恢复过程中由于主接口状态为 down，因此主接口上的路由不可达，导致备份链路被呼叫。配置恢复后，所有接口的状态变为 up，备份链路被呼叫成功，此时由于主接口路由恢复，备份链路再次被禁用，状态变为 down。为了避免系统启动后的短时间内备份链路 up/down 切换一次，可以配置在系统启动指定时间后动态路由备份功能才生效，在这段时间内不对备份链路进行呼叫

4.3.8 通过轮询 DCC 中的接口备份和 3G 网络实现干线链路备份的配置示例

本示例的基本网络结构如图 4-11 所示，RouterA 是某企业的出口网关。正常情况下，RouterA 通过 ADSL 接口接入 IP 网络（假设是以 PPPoA 专线 ADSL 方式接入）。为了防止当 ADSL 接口出现故障从而导致企业用户无法连接到 IP 网络的情况，该企业通过备份接口（即图中的 3G 接口）接入 IP 网络。通过对企业出口接口的备份，增强了线路的可靠性。

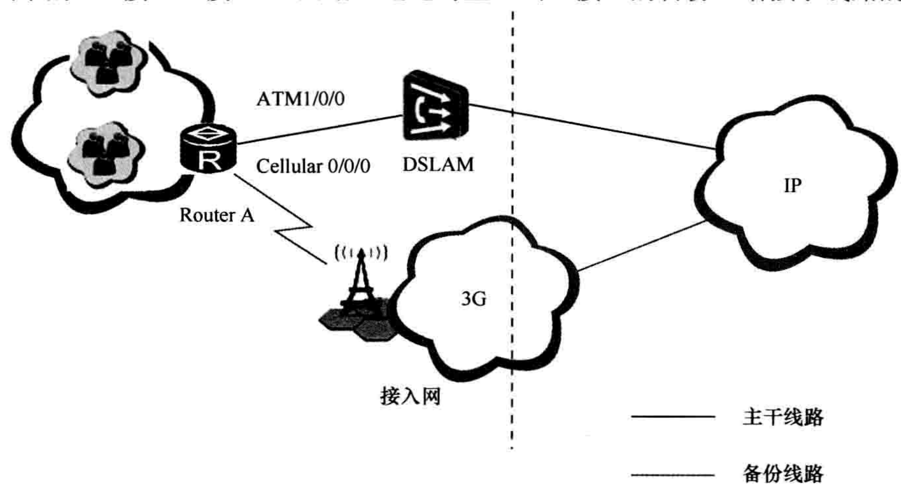


图 4-11 轮询 DCC 中通过接口备份和 3G 网络实现干线链路备份配置示例的基本网络结构

1. 配置思路

本示例的要求很明确，也很简单，就是要配置一条用于备份 ADSL 上行线路的 3G 上行备份线路。从整体网络配置角度来看，需要做以下几方面的配置。

① 配置企业内网，指定 RouterA 的 LAN 口 IP 地址作为内网主机默认网关，具体配置略。

② 配置 RouterA 的上行 ADSL 主用接口。

ADSL 接口方面大家可以参见本书第 3 章 3.12.5 小节介绍的配置示例中的 ADSL 接口配置。因为本示例中主接口采用的是 PPPoA 专线 ADSL 接入方式，需要承载 ATM 业务，所以需要创建应用 ATM 协议的 VT（虚拟模板）接口，并指定 3G cellular 接口作为 VT 的备份接口。

③ 配置 RouterA 的上行 3G 备份接口。

这是本示例要介绍的配置任务。假设对接的 3G 网络为 WCDMA 网络，现要接入 WCDMA 的 PS 域，需要配置拨号串为“*99#”。APN 的名称需要和运营商给定的一致，现假设接入的 APN 名称为“wcdma”。配置备份接口前，请确保 3G modem 和 SIM/UIM 卡都在位。

④ 配置两条通过不同上行接口，不同优先级的缺省路由，使得 3G 线路成为 ADSL 线路的备份线路。

2. 具体配置步骤

本示例以上后面三项配置任务的具体配置步骤如下（不包括 ADSL 接口的配置）。

① 配置 RouterA 的上行主用接口。有关接口备份配置将在本书后面介绍。

```
[RouterA] acl number 3002
[RouterA-acl-adv-3002] rule 5 permit ip source 192.168.100.0 0.0.0.255        !---配置允许内网通过 NAT 接入 IP 网络的 ACL
[RouterA-acl-adv-3002] quit
[RouterA] interface virtual-template 10                    !---创建虚拟模板接口 10
[RouterA-Virtual-Template10] ip address ppp-negotiate      !---配置 VT 10 接口采用自动方式获取 IP 地址
[RouterA-Virtual-Template10] nat outbound 3002             !---在 VT10 接口出方向上应用前面配置的 ACL 3002
[RouterA-Virtual-Template10] quit
[RouterA] interface atm 1/0/0                              !---进入 ADSL 接口
[RouterA-Atm1/0/0] pvc voip 1/35                           !---根据指定 ADSL 线路中的 VPI/VCI 值
[RouterA-atm-pvc-Atm1/0/0-1/35-voip] map ppp virtual-template 10   !---将 ADSL 接口映射到 VT10 上
[RouterA-atm-pvc-Atm1/0/0-1/35-voip] quit
[RouterA-Atm1/0/0] standby interface cellular 0/0/0        !---指定 3G cellular 0/0/0 为 ADSL 接口的备份接口
[RouterA-Atm1/0/0] standby timer delay 10 10     !---指定主接口到备份接口，以及备份接口到主接口的切换时间均为 10 s
[RouterA-Atm1/0/0] quit
```

② 配置 RouterA 的上行备份接口。

```
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit              !---配置允许 IP 访问的拨号访问规则
[RouterA-dialer-rule] quit
[RouterA] interface cellular 0/0/0
[RouterA-Cellular0/0/0] profile create 1 static wcdma  !---创建 3G modem 的参数描述模板，并创建名为 wcdma 的用户
手工 APN
[RouterA-Cellular0/0/0] link-protocol ppp
[RouterA-Cellular0/0/0] ip address ppp-negotiate
[RouterA-Cellular0/0/0] dialer enable-circular
[RouterA-Cellular0/0/0] dialer-group 1                     !---指定 3G Cellular0/0/0 接口属于 1 号拨号访问组
[RouterA-Cellular0/0/0] dialer timer idle 0                !---设定当 3G Cellular0/0/0 接口的 DCC 轮询呼叫建立后，允许链
```

路空闲的时间为 0 s，即不等待

```
[RouterA-Cellular0/0/0] dialer number *99#    !---配置 3G Cellular0/0/0 接口向 ISP 局端 DCC 轮询拨号的拨号串中为*99#
[RouterA-Cellular0/0/0] nat outbound 3002     !---在 3G Cellular0/0/0 接口出方向上应用前面配置的 ACL3002
[RouterA-Cellular0/0/0] quit
```

③ 配置两条优先级不一样的缺省路由。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 virtual-template 10    !---配置以 VT10 接口为出接口的缺省路由为主缺省路由，因为它的优先级设为比静态路由缺省优先级 60 更高的优先级 10
[RouterA] ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/0    !---配置以 3G Cellular0/0/0 接口为出接口的缺省路由为备份缺省路由，因为它采用优先级更低的缺省优先级 60
```

4.4 配置共享 DCC

共享 DCC 中一个物理接口可以属于多个 Dialer bundle（拨号捆绑），服务于多个 Dialer 接口；但一个 Dialer 接口只对应一个目的地址，只能使用一个 Dialer bundle；一个 Dialer bundle 中可以包含多个物理接口，每个物理接口具有不同的优先级。

支持共享 DCC 的物理接口包括：ADSL 接口、G.SHDSL 接口、VDSL 接口、E1-IMA 接口、WAN 侧以太网接口、ISDN PRI 接口和 ISDN BRI 接口。

总体来说，共享 DCC 的配置任务与前面介绍的轮询 DCC 的配置任务差不多，但因为共享 DCC 中一个 Dialer 接口中只能配置一个目的地址，所以没有 4.3.6 小节的拨号串循环备份功能。共享 DCC 的主要配置任务如下（**必需的只是前面三项**）。

① 配置链路层协议和 IP 地址。

② 使能共享 DCC 并配置 DCC 拨号 ACL 及与接口的关联。

③ 配置共享 DCC 呼叫。

④（可选）配置 DCC 拨号接口属性。

⑤（可选）配置 DCC 呼叫 MP 捆绑。

⑥（可选）配置通过 DCC 实现动态路由备份。

注意 共享 DCC 中的 DCC 参数（包括拨号接口属性）配置只能在 Dialer 接口上配置，不能在物理拨号接口上配置。

因为共享 DCC 中以上各项配置任务中的许多配置与轮询 DCC 的对应配置任务的配置方法差不多，故在此一并进行介绍。

1. 配置链路层协议和 IP 地址

共享 DCC 中的具体链路层协议和 IP 地址配置方法与轮询 DCC 中的链路层协议和 IP 地址配置方法完全一样，参见 4.3.1 小节的表 4-2。只是对于共享 DCC，如果是主叫端，需在 Dialer 接口下配置 PPP 的相关命令，但建议用户在物理拨号接口下也配置相同的 PPP 相关命令，以确保 PPP 链路参数协商的可靠性；如果是被叫端，需在物理拨号接口下配置 PPP 相关命令。

说明 对于 ISDN PRI、ISDN BRI 接口，当采用共享 DCC 时，B 通道初始封装为 PPP，一旦该 B 通道被选用，其封装协议跟随 Dialer 接口链路层协议动态改变，使得 B 通道能

够被封装不同链路协议的 Dialer 接口所选用，确保了灵活性。当该 B 通道被释放，其封装协议自动恢复为 PPP。

2. 使能共享 DCC 并配置 DCC 拨号 ACL 及与接口的关联

在共享 DCC 中，使能共享 DCC、配置 DCC 拨号 ACL 及与接口的关联仅可在 Dialer 接口下配置，不能在物理拨号接口下配置。具体配置步骤如表 4-9 所示。

表 4-9　使能共享 DCC 并配置 DCC 拨号 ACL 及与接口关联的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dialer-rule** 例如：[Huawei] **dialer-rule**	进入 Dialer-rule 视图
3	**dialer-rule** *dialer-rule-number* { **acl** { *acl-number* | **name** *acl-name* } | **ip** { **deny** | **permit** } | **ipv6** { **deny** | **permit** } } 例如：[Huawei-dialer-rule] **dialer-rule** 1 **ip permit**	配置某个拨号访问组对应的拨号访问控制列表，指定引发 DCC 呼叫的条件。其他说明参见 4.3.2 小节中表 4-3 中的第 3 步
4	**quit** 例如：[Huawei-dialer-rule] **quit**	退出 Dialer-rule 视图，返回系统视图
5	**interface dialer** *interface-number* 例如：[Huawei] **interface dialer** 0	进入 Dialer 接口视图 如果要在物理拨号接口上配置，则使用 **interface** *interface-type interface-number* 命令进入相应的接口视图
6	**dialer user** *username* 例如：[Huawei-Dialer0] **dialer user** winda	在 Dialer 接口上使能共享 DCC 功能。参数 *username* 用来指定对端用户名，1～32 个字符，**不支持空格，区分大小写**，但该用户名必须与对端配置的 PPP 用户名一致 【注意】在一个 Dialer 接口视图下多次执行本命令，新的配置不会覆盖老的配置。多次配置的结果是该 Dialer 接口和多个对端用户对应 缺省情况下，共享 DCC 处于去使能状态且没有配置对端用户名，可用 **undo dialer user** [*user-name*]命令去使能共享 DCC 并删除已经配置的对端用户名，如果不指定 *user-name* 可选参数，则去使能共享 DCC 且删除所有已经配置的对端用户名
7	**dialer bundle** *number* 例如：[Huawei-Dialer0] **dialer bundle** 1	指定以上共享 DCC 的 Dialer 接口使用的 Dialer bundle(拨号捆绑)，取值范围为 1～255 的整数。Dialer bundle 是用指定有哪些物理端口进行捆绑与一个 Dialer 接口对应的，但一个 Dialer 接口只能对应一个 Dialer bundle 缺省情况下，Dialer 接口没有对应的 Dialer bundle，可用 **undo dialer bundle** 命令删除共享 DCC 的对应 Dialer 接口使用的 Dialer bundle
8	**dialer-group** *group-number* 例如：[Huawei-Dialer0] **dialer-group** 1	配置以上 Dialer 接口的拨号访问组。其他说明参见 4.3.2 小节中表 4-3 中的第 7 步

3. 配置共享 DCC 呼叫

使用共享 DCC 实现按需拨号时，由于物理接口随着拨号串的不同而具有不同属性，因此必须在 Dialer 接口上配置 DCC 参数，并且只能使用 **dialer number** 命令配置呼叫对

端的拨号串。一个 Dialer 接口只能配置一个拨号串。具体配置步骤如表 4-10 所示。

表 4-10 共享 DCC 呼叫的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface dialer** *interface-number* 例如：[Huawei] **interface dialer** 0	进入 Dialer 接口视图
3	**dialer number** *dial-number* [**autodial**] 例如：[Huawei-Dialer0] **dialer number** 12345	在 Dialer 接口上配置呼叫一个对端的拨号串 【注意】如果拨号接口的 IP 地址配置为接受 PPP 协商产生的由对端分配的 IP 地址，此处需要使用本命令来指定拨号串，不能使用下面的 **dialer route ip** 命令 使用共享 DCC，**主叫端不同拨号接口允许存在重复的拨号串配置，被叫端拨号串的配置不能重复** 设备支持在同一个拨号接口下多次执行本命令配置呼叫一个对端的多个拨号串，但如果选择 **autodial** 可选项，那么该拨号接口只能执行一次 **dialer number** 命令配置呼叫一个对端的拨号串 其他说明参见 4.3.3 小节表 4-4 中的第 3 步
4	**quit** 例如：[Huawei-Dialer0] **quit**	退出 Dialer 接口视图，返回系统视图
5	**interface** *interface-type interface-number* 例如：[Huawei] **interface** serial 1/0/0:15	键入要绑定在与以上 Dialer 接口对应的 Dialer bundle 的物理拨号接口，进入相应的接口视图
6	**dialer bundle-member** *number* [**priority** *priority*] 例如：[Huawei-Serial1/0/0:15] **dialer bundle-member** 1 **priority** 50	把以上物理拨号接口加入指定的 Dialer bundle 中，并为它设置优先级。命令中的参数说明如下 ● *number*：指定以上物理拨号接口要加入的 Dialer bundle 编号，取值范围为 1～255 的整数 ● *priority*：可选参数，指定物理接口在这个 Dialer bundle 中的优先级，取值范围为 1～255 的整数。数值越大表示优先级越高。拨号过程中，优先选择优先级高的物理接口 【说明】因为在共享 DCC 中，同一个 Dialer bundle 中的多个物理接口是拨号访问同一个目的地址的，所以可以为这些物理拨号接口配置不同的拨号优先级 在同一个视图下多次执行本命令，新配置不会覆盖旧配置。多次配置的结果是一个物理接口属于多个 Dialer bundle 缺省情况下，物理接口不属于任何 Dialer bundle，可用 **undo dialer bundle-member** *number* 命令将本地物理接口脱离指定的 Dialer bundle。

4. 配置 DCC 拨号接口属性

这部分的配置与 4.3.4 小节介绍的 DCC 拨号接口属性配置完全一样，参见表 4-6。要注意的是，这里仅可以在 Dialer 接口上配置。

5. 配置 DCC 呼叫 MP 捆绑

这部分的配置与 4.3.5 小节介绍的 DCC 呼叫 MP 捆绑配置完全一样，参见表 4-7 即可。

6. 配置通过 DCC 实现动态路由备份

这部分的配置与 4.3.7 小节介绍的通过 DCC 实现动态路由备份的配置完全一样，参见表 4-8。要注意的是，这里仅可以在 Dialer 接口上配置。

4.5 DCC 管理

配置好 DCC 后，可以通过以下 **display** 任意视图命令查看相关配置信息和拨号接口状态，也可通过以下 **reset** 用户视图命令清除拨号接口上的统计信息。

① **display dialer** [**interface** *interface-type interface-number*]：查看拨号接口（可以在物理拨号接口中，也可以上 Dialer 接口）的 DCC 信息，包括拨号接口的相关参数，这些信息可以帮助用户分析 DCC 拨号的过程，有助于故障解决。

② **display interface dialer** [*number*]：查看 Dialer 接口的信息，包括 Dialer 接口的状态信息和统计信息。用户可以根据这些信息进行流量统计和接口的故障诊断等。

③ **reset counters interface** [**dialer** [*number*]]：清除 Dialer 接口统计信息后，以前的统计信息将无法恢复。

如果为了缓解网络压力或调整拨号配置需要临时拆除拨号链路时，可以通过 **dialer disconnect** [**interface** *interface-type interface-number*]任意视图命令手动拆除拨号链路。但本命令只是临时拆除拨号链路：如果被拆除的拨号链路配置了自动拨号，当达到自动拨号时间时，会重新建立拨号链路；如果被拆除的拨号链路未配置自动拨号，则当有报文需要传输时，会再次触发拨号。

4.6 PPP 配置与管理

PPP 是在点到点链路上承载网络层数据报文的一种链路层协议，如路由器中的 Serial 接口链路缺省运行的协议就是 PPP。当然，能够运行 PPP 的远不止 Serial 这一种接口，如 Async 接口、CPOS 接口、ISDN BRI 接口、E1-F 接口、CE1/PRI 接口、T1-F 接口、CT1/PRI 接口、3G Cellular 接口、Dialer 接口、虚拟模板接口、POS 接口等都可以运行 PPP。

4.6.1 PPP 简介及基本工作机制

PPP 是在 SLIP（Serial Line Internet Protocol，串行线 IP）的基础上发展起来的。由于 SLIP 具有只支持异步传输方式、无协商过程（尤其不能协商如双方 IP 地址等网络层属性）、只能承载 IP 一种网络层报文等缺陷，在发展过程中，逐步被 PPP 替代。

由于 PPP 能够提供用户认证、易于扩充，并且支持同/异步通信，因而获得广泛应用。配置 PPP 可以实现 PPPoE、PPPoA、PPPoEoA 拨号上网及广域网互联，提供包括 PPPoE、PPPoA、PPPoEoA、PPPoFR 和 PPPoISDN 等多种业务。PPP 还可以运用于专线网络，实现企业总部与分支之间通过 DDN 网络进行对接。

相对其他链路层协议来说，PPP 有如下优点。

① 对物理层而言，PPP 既支持同步链路又支持异步链路，而 X.25、FR（Frame Relay）等数据链路层协议仅支持同步链路，SLIP 仅支持异步链路。

② PPP 具有良好的扩展性，例如，当需要在以太网链路上承载 PPP 时，PPP 可以扩展为 PPPoE。

③ 提供 LCP（Link Control Protocol，链路控制协议），主要用来建立、拆除和监控 PPP 数据链路。

④ 提供各种 NCP（Network Control Protocol，网络控制协议）（如 IPCP、IPXCP），主要用来协商在该数据链路上所传输的数据包的格式与类型，更好地支持了网络层协议。

⑤ 提供认证协议 CHAP（Challenge-Handshake Authentication Protocol，质询握手认证协议）、PAP（Password Authentication Protocol，密码认证协议），主要用于网络安全方面的认证，更好地保证了网络的安全性。

⑥ 无重传机制，网络开销小，速度快。

以上 LCP、NCP、CHAP/PAP 就是 PPP 所包含的三大扩展子协议，而 PPP 的工作机制正是在这三大扩展子协议协同工作基础上实现的。

整个 PPP 运行流程分为 5 个阶段，即 Dead（死亡）阶段、Establish（链路建立）阶段、Authenticate（身份认证）阶段、Network（网络控制协商）阶段和 Terminate（结束）阶段。不同阶段进行不同协议的协商，只有前面的协议协商出结果后，才能转入下一个阶段协议的协商，如图 4-12 所示。具体流程如下。

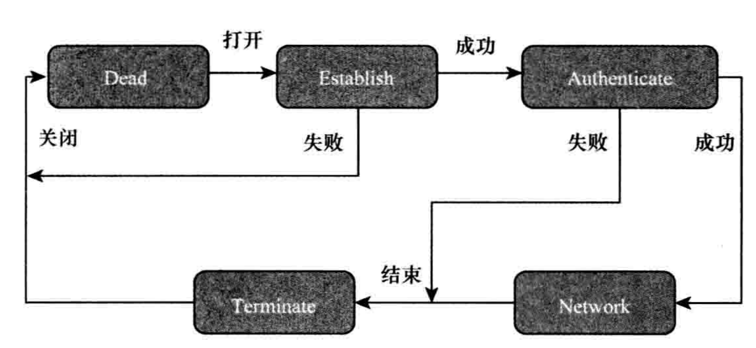


图 4-12 PPP 运行基本流程

① 当有用户向 ISP 或者对端节点发起 PPP 连接请求时，首先打开物理接口，然后 PPP 在建立链路之前先通过封装了 LCP 的 PPP 帧与接口进行协商，协商内容包括工作方式是 SP（单 PPP 通信），还是 MP（多 PPP 通信），认证方式和最大传输单元等。

② LCP 协商完成后就进入 Establish 阶段，进行数据链路建立。这时主要启用 PPP 数据链路层协议，对接口进行封装。如果启用成功，则进入身份认证（Authenticate）阶段，并保持 LCP 为激活状态，否则返回关闭接口，LCP 的状态转换为 Down。

③ 如果数据链路建立成功，进入 Authenticate 阶段，对请求连接的用户进行身份认证。具体要根据通信双方所配置的身份认证方式来确定是采用 CHAP，还是 PAP 身份

认证。

④ 如果认证成功就进入 Network 阶段，使用封装了 NCP 的 PPP 帧与对应的网络层协议进行协商，并为用户分配一个临时的网络层地址（如 IP 地址）；如果身份认证失败，则直接进入 Terminate（结束）阶段，拆除链路，返回到 Dead 阶段，LCP 状态转换为 Down。

⑤ PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（如用户的干预），进入到 Terminate 阶段，然后关闭 NCP 协议，释放原来为用户分配的临时网络层地址，最后返回到 Dead 阶段，关闭 LCP。

4.6.2　配置 PPP 基本功能

PPP 基本功能包括配置接口的链路层协议为 PPP 和配置端口的 IP 地址。通信双方的 PPP 基本功能配置完成后，可以初步建立 PPP 链路。主要包括以下两项配置任务。

（1）配置接口封装的链路层协议为 PPP

这步其实不用配置，因为除以太网接口外，其他接口封装的链路层协议均为 PPP。

（2）配置接口的 IP 地址

配置接口的 IP 地址主要有两种方式：一种是在接口上直接配置 IP 地址，另一种是通过 IP 地址协商获取 IP 地址。配置 PPP 协商 IP 地址又分以下两种情况。

① 配置设备作为 PPP 客户端

如果本端设备接口封装的链路层协议为 PPP，且未配置 IP 地址，而对端已有 IP 地址时，可把本端设备配置为客户端，使本端设备接口接收 PPP 协商产生的由对端分配的 IP 地址。这种方式主要用在通过 ISP 访问 Internet 时，获得由 ISP 分配的 IP 地址。

② 配置设备作为 PPP 服务器

设备作为服务器时可以为对端设备指定 IP 地址，但首先要在系统视图下配置本地 IP 地址池，指明地址池的地址范围，然后在接口视图下指定该接口使用的地址池。

具体配置步骤如表 4-11 所示。

表 4-11　　PPP 基本功能配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	进入接口视图，可以是 Serial 接口、Async 接口、CPOS 接口、ISDN BRI 接口、E1-F 接口、CE1/PRI 接口、T1-F 接口、CT1/PRI 接口、3G Cellular 接口、Dialer 接口、虚拟模板接口、POS 接口
3	**link-protocol ppp** 例如：[Huawei-Serial1/0/0]**link-protocol ppp**	配置接口封装的链路层协议为 PPP 缺省情况下，除以太网接口外，其他接口封装的链路层协议均为 PPP
方式 1：设备作为 PPP 客户端时为自己配置 IP 地址		
4	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**] 例如：[Huawei-Serial1/0/0] **ip address** 192.168.1.2 24	（二选一）直接为接口配置 IP 地址

（续表）

步骤	命令	说明
4	**ip address ppp-negotiate** 例如：[Huawei-Serial1/0/0] **ip address ppp-negotiate**	（二选一）配置接口通过 PPP 协商获取 IP 地址，但必须确保对端接口已配置了 IP 地址 【说明】如果本端接口封装的链路层协议为 PPP，但还未配置 IP 地址，而对端已有 IP 地址时，可为本端接口配置 IP 地址可协商属性，使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。这种方式主要用在通过 ISP 访问 Internet 时，获得由 ISP 分配的 IP 地址 缺省情况下，接口不通过 PPP 协商获取 IP 地址，可用 **undo ip address ppp-negotiate** 命令取消接口通过 PPP 协商获取 IP 地址
方式 2：设备作为 PPP 服务器时为对端设备配置 IP 地地址		
4	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-Serial1/0/0] **ip address** 192.168.1.1 24	配置服务器设备的 IP 地址，因已在本书中多次介绍，故不再赘述
5	**remote address** *ip-address* 例如：[Huawei-Serial1/0/0] **remote address** 192.168.1.2 24	（二选一）配置直接为对端分配 IP 地址。参数 *ip-address* 用来指定为对端分配的 IP 地址 此时需要在作为客户端的设备上配置上面第 3 步中的 **ip address ppp-negotiate** 命令，以使对端接口接受由 PPP 协商产生的分配的 IP 地址 缺省情况下，本端不为对端分配 IP 地址，可用 **undo remote address** 命令恢复缺省值
	remote address pool *pool-name* 例如：[Huawei-Serial1/0/0] **remote address pool** global1	（二选一）配置采用 DHCP 全局地址池为对端分配 IP 地址。参数 *pool-name* 用来指定为对端分配 IP 地址的地址池名称，将指定地址池中的一个 IP 地址分配给对端，1～64 个字符，不支持空格，区分大小写 缺省情况下，本端不为对端分配 IP 地址，可用 **undo remote address** 命令恢复缺省值
6	**ppp ipcp remote-address forced** 例如：[Huawei-Serial1/0/0] **ppp ipcp remote-address forced**	（可选）使本设备为对端分配的 IP 地址具有强制性，不允许对端使用自行配置的 IP 地址，它必须与上一步的 **remote address** 配合使用 缺省情况下，在 PPP 的 IPCP 协商阶段进行 IP 地址协商时，IP 地址协商情况为本端不具有地址分配的强制性，即本端设备允许对端自行配置 IP 地址，可用 **undo ppp ipcp remote-address forced** 命令取消这种强制性，允许对端使用自行配置的 IP 地址
7	**quit** 例如：[Huawei-Serial1/0/0] **quit**	退出接口视图，返回系统视图
8	**ip pool** *ip-pool-name* 例如：[Huawei] **ip pool** global1	（可选）创建全局地址池，仅当在第 5 步中采用了 DHCP 服务器全局地址池为对端分配 IP 地址时才需要配置。参数 *ip-pool-name* 用来指定地址池名称，1～64 个字符，不支持空格，区分大小写 缺省情况下，没有创建全局地址池，可用 **undo ip pool** *ip-pool-name* 命令删除指定的全局地址池

（续表）

步骤	命令	说明
9	**network** *ip-address* [**mask** { *mask* | *mask-length* }] 例如：[Huawei-ip-pool-global1] **network** 192.1.1.0 **mask** 24	（可选）配置全局地址池下可分配的网段地址，仅当在第 5 步中采用了 DHCP 服务器全局地址池为对端分配 IP 地址时才需要配置。命令中的参数说明如下 • *ip-address*：指定全局地址池中的 IP 地址段，是一个网络地址，**不是一个主机 IP 地址** • **mask** { *mask* | *mask-length* }：可选参数，指定以上 IP 地址段所对应的子网掩码（选择 *mask* 参数时）或子网掩码长度（选择 *mask-length* 参数时） 缺省情况下，系统未配置全局地址池下动态分配的 IP 地址范围，可用 **undo network** 命令恢复网段地址为缺省值

4.6.3　配置 PPP 的 PAP 认证

PPP 基本功能实现后，用户根据需要配置 PAP 或 CHAP 认证。

① PAP 认证：这是一种两次握手验证协议。**它是以明文方式在链路上发送验证密码，**完成 PPP 链路建立后，被验证方会不停地在链路上反复发送用户名和密码，直到身份验证过程结束，所以安全性不高。

② CHAP 认证：这是一种三次握手验证协议。**它只在网络上传输用户名，而不传输用户密码，**因此安全性比 PAP 认证高。

本节介绍 PPP 的 PAP 认证配置方法，下节将介绍 PPP 的 CHAP 认证的配置方法。有关 PAP 或 CHAP 认证原理可参见其他相关专业图书。

PAP 认证分为 PAP 单向认证与 PAP 双向认证：PAP 单向认证是指一端作为认证方，另一端作为被认证方；双向认证是单向认证的简单叠加，即两端都是既作为认证方又作为被认证方。在配置 PPP 的 PAP 认证之前，需完成上节介绍的 PPP 基本功能配置。

【经验之谈】PAP 认证需要同时在认证方（实施认证的一方）和被认证方进行配置。在认证方本地要创建好用于对被认证方进行认证的用户账户信息（包括用户名和密码），而在被认证方要配置在进行认证时要发送的用户账户信息，且要与认证方本地用于认证的用户账户信息完全一致。当然，两端还要配置采用相同的 PPP 认证方式。

表 4-12 所示为一个方向的 PAP 认证配置方法，如果要进行双向 PAP 认证，则要在两端设备上同时配置表中的认证方和被认证方，**不同方向的认证所采用的认证账户信息可以一样，也可以不一样。**

表 4-12　　PPP 的 PAP 认证配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	进入接口视图，可以是 Serial 接口、Async 接口、CPOS 接口、ISDN BRI 接口、E1-F 接口、CE1/PRI 接口、T1-F 接口、CT1/PRI 接口、3G Cellular 接口、Dialer 接口、虚拟模板接口、POS 接口

（续表）

步骤	命令	说明
		在认证方设备上配置认证方式
3	**ppp authentication-mode pap** [[**call-in**] **domain** *domain-name*] 例如：[Huawei-Serial1/0/0] **ppp authentication-mode pap domain** lycb	配置本端设备对对端设备采用 PAP 认证方式。命令中的参数和选项说明如下 ● **call-in**：可选项，指定只在远端用户呼入时才认证对方 ● **domain** *domain-name*：可选参数，指定用户认证采用的域名，1～64 个字符，支持空格，**但区分大小写，且不能使用星号“*”、问号“?”、引号“"”等**。如果不指定域，则以对端发送的用户名中带的域认证用户；如果对端发送的用户名中也不包含域，则使用缺省域 default 认证用户 缺省情况下，PPP 协议不进行认证，可用 **undo ppp authentication-mode** 命令恢复为缺省情况
4	**quit** 例如：[Huawei-Serial1/0/0] **quit**	退出接口视图，返回系统视图
5	**aaa** 例如：[Huawei] **aaa**	进入 AAA 视图
6	**local-user** *user-name* **password cipher** *password* 例如：[Huawei-aaa] **local-user** winda **password cipher** huawei	创建本地用户的用户名和密码。命令中的参数说明如下 ● *user-name*：指定用于认证的本地用户名，1～64 个字符，**不支持空格，区分大小写**，格式“user@domain”。查询与修改时可以使用通配符“*”，例如*@isp、user@*、*@*。如果用户名中带域名分隔符，如@，则认为@前面的部分是用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域为默认域 ● *password*：指定以上本地用户的密码，**不支持空格，区分大小写**，明文形式下是 1～32 个字符，密文形式下是 32～56 个字符。**cipher** 表示以密文形式显示用户密码，并且在查看配置文件时将以密文方式显示密码。如果未指定该参数，设备会自动为该用户指定一个缺省的密码 vlan 【说明】这里仅以缺省域下 AAA 本地认证方式进行介绍，关于 RADIUS 认证及 HWTACACS 认证的相关配置请参见配套的《华为交换机学习指南》第 17 章 缺省情况下，系统中存在一个名称为“admin”的本地用户，该用户的密码为“vlan”，优先级为 15，可用 **undo local-user** *user-name* 命令删除指定的本地用户
7	**local-user** *user-name* **service-type ppp** 例如：[Huawei-aaa] **local-user** winda **service-type ppp**	配置参数 *user-name* 指定的本地用户（**要与上一步配置的用户名一致**）使用的服务类型为 PPP 缺省情况下，本地用户可以使用所有的接入类型，可用 **undo local-user** *user-name* **service-type** 命令将指定的本地用户的接入类型恢复为缺省配置
		在被认证方设备上配置认证方式
3	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password* 例如：[Huawei-Serial1/0/0] **ppp pap local-user** winda **cipher** huawei	配置本地被对端以 PAP 方式认证时本地发送的 PAP 用户名和密码。命令中的参数和选项说明如下 ● *username*：指定本地设备被对端设备采用 PAP 方式认证时发送的用户名，1～64 个字符，**不支持空格，区分大小写，要与认证方配置的用户名一致**

（续表）

步骤	命令	说明
3	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password* 例如：[Huawei-Serial1/0/0] **ppp pap local-user** winda **cipher** huawei	• **cipher**：二选一选项，指定密码为密文显示 • **simple**：二选一选项，指定密码为明文显示 • *password*：指定本地设备被对端设备采用 PAP 方式认证时发送的密码，支持空格，区分大小写，如果选择 **simple** 选项，则必须是 1～32 个字符的明文密码；如果选择 **cipher** 选项，则既可以是 24～56 个字符的密文密码，也可以是 1～32 个字符的明文密码，**但要与认证方配置的密码一致** 缺省情况下，对端采用 PAP 认证时本地设备发送的用户名和密码均为空，可用 **undo ppp pap local-user** 命令取消配置的用户名和密码

注意　在认证方或者被认证方完成上述 PAP 认证配置后，必须在对应的接口视图下依次执行 **shutdown** 和 **undo shutdown** 重启接口，PAP 认证才能生效。

4.6.4　配置 PPP 的 CHAP 认证

CHAP 认证也分为 CHAP 单向认证与 CHAP 双向认证两种。CHAP 单向认证是指一端作为认证方，另一端作为被认证方；双向认证是单向认证的简单叠加，即两端都是既作为认证方又作为被认证方。另外，CHAP 认证过程分为两种情况：认证方配置了用户名和认证方没有配置用户名。推荐使用认证方配置用户名的方式，这样可以对认证方的资格进行确认。

【经验之谈】当认证方配置了用户名时，可以使被认证方验证认证方的资格，以防连接到非法的服务器端。也就是被认证方也有资格验证对方是否有资格对自己进行认证。就相当于一个双向认证：不仅认证方可以对被认证进行认证，被认证方也可对认证方进行认证，这就是 CHAP 三次握手过程的基本原理。在认证方没有配置用户名时，CHAP 认证过程就与前面介绍的 PAP 认证过程完全一样，仅是一个认证方对被认证方进行的单向认证。但要注意，**这里所说的“单向认证”和“双向认证”与前面所说的 PAP 和 CHAP 都支持“单向认证”和“双向认证”是不同的**，这里的是针对同一次会话活动而言的，而 PAP 和 CHAP 中所支持的“单向认证”和“双向认证”则是针对两次会话活动而言的。

在配置 PPP 的 PAP 认证之前，需完成上节介绍的 PPP 基本功能配置。

认证方配置了用户名后的 CHAP 认证具体配置步骤如表 4-13 所示。**双方都要配置认证用户名，创建用于对方认证的本地用户名账户**，因为此时被认证方同时需要对认证的资格进行确认，适用于安全性较高的环境。认证方没有配置用户名的 CHAP 认证的具体配置步骤如表 4-14 所示，此时**被认证方不需要对认证的资格进行确认**，适用于安全性较好的环境。但表中所列的都仅是针对 CHAP 单向认证进行介绍的，**双向认证时需要双方同时配置表中的认证方和被认证方**。

表 4-13 认证方配置了用户名时的 CHAP 认证具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	进入接口视图，其他说明参见上节表 4-12 中的第 2 步
认证方配置了用户名时的认证方配置		
3	**ppp authentication-mode chap** [[**call-in**] **domain** *domain-name*] 例如：[Huawei-Serial1/0/0] **ppp authentication-mode chap domain** lycb	配置本端设备对对端设备采用 CHAP 认证方式。命令中的参数和选项说明参见上节表 4-12 中认证方设备上配置的第 3 步
4	**ppp chap user** *username* 例如：[Huawei-Serial1/0/0] **ppp chap user** grfw	设置 CHAP 认证的用户名。参数 *username* 用来指定发送到被认证方设备进行 CHAP 验证时使用的用户名（使被认证方确认认证方资格，**不需要在认证方本地创建**），1～64 个字符，**不支持空格，区分大小写。在被认证方上为认证方配置的本地用户的用户名必须与此处配置的一致**，即与本表下面被认证方设备上配置的第 6 步通过 **local-user** 命令创建的用户名一致 【说明】因为 CHAP 认证中只发送用户名，所以可不需要配置密码，也可使用 **ppp chap password** { **cipher** | **simple** } *password* 命令为对应的配置配置用户密码 缺省情况下，CHAP 认证的用户名为空，可用 **undo ppp chap user** 命令删除 CHAP 认证的用户名
5	**quit** 例如：[Huawei-Serial1/0/0] **quit**	退出接口视图，返回系统视图
6	**aaa** 例如：[Huawei] **aaa**	进入 AAA 视图
7	**local-user** *user-name* **password cipher** *password* 例如：[Huawei-aaa] **local-user** winda **password cipher** huawei	创建本地用户的用户名和密码，这是用来对被认证方所发送的用户名进行认证的用户信息，**需要在认证方本地创建。这里配置的用户名要与被认证方配置的认证用户名一致**，即与本表下面被认证方设备配置的第 3 步通过 **ppp chap user** 命令配置的用户名一致。命令中的参数说明参见上节表 4-12 中认证方设备上配置的第 6 步
8	**local-user** *user-name* **service-type ppp** 例如：[Huawei-aaa]**local-user** winda **service-type ppp**	配置参数 *user-name* 指定的本地用户（**要与上一步配置的用户名一致**）使用的服务类型为 PPP。其他说明参见上节表 4-12 中认证方设备上配置的第 7 步
认证方配置了用户名时的被认证方配置		
3	**ppp chap user** *username* 例如：[Huawei-Serial1/0/0]**ppp chap user** winda	设置 CHAP 认证的用户名。参数 *username* 用来指定被认证方向认证方发送的用户名（用于认证方对被认证方的认证，**不需要在被认证方本地创建**），在认证方上为被认证方配置的本地用户的用户名必须与此处配置的一致，即与本表下面认证方设备配置的第 7 步通过 **local-user** 命令创建的用户名一致。其他说明参见本表认证方设备配置的第 4 步

（续表）

步骤	命令	说明
4	**quit** 例如：[Huawei-Serial1/0/0] **quit**	退出接口视图，返回系统视图
5	**aaa** 例如：[Huawei] **aaa**	进入 AAA 视图
6	**local-user** *user-name* **password cipher** *password* 例如：[Huawei-aaa] **local-user** grfw **password cipher** huawei1234	创建本地用户的用户名和密码，用于验证认证方的资格，**需要在被认证方本地创建**。这里创建的用户名要和认证方配置的认证用户名一致，即与本表上面认证方设备配置的第 4 步通过 **ppp chap user** 命令配置的用户名一致。命令中的参数说明参见**上节表 4-12 中认证方设备上配置的第 6 步**
7	**local-user** *user-name* **service-type ppp** 例如：[Huawei-aaa] **local-user** grfw **service-type ppp**	配置参数 *user-name* 指定的本地用户（**要与上一步配置的用户名一致**）使用的服务类型为 PPP。其他说明参见上节表 4-12 中认证方设备上配置的第 7 步

表 4-14　　认证方没有配置用户名时的 CHAP 认证具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	进入接口视图，其他说明参见上节表 4-12 中的第 2 步
认证方没有配置用户名时的认证方配置		
3	**ppp authentication-mode chap** [[**call-in**] domain *domain-name*] 例如：[Huawei-Serial1/0/0]**ppp authentication-mode chap domain** lycb	配置本端设备对对端设备采用 CHAP 认证方式。命令中的参数和选项说明参见上节表 4-12 中认证方设备配置的第 3 步
4	**quit** 例如：[Huawei-Serial1/0/0] **quit**	退出接口视图，返回系统视图
5	**aaa** 例如：[Huawei] **aaa**	进入 AAA 视图
6	**local-user** *user-name* **password cipher** *password* 例如：[Huawei-aaa] **local-user** winda **password cipher** huawei	创建本地用户的用户名和密码，这是用来对被认证方所发送的用户名进行认证的用户信息，**需要在认证方本地创建。这里配置的用户名要与被认证方配置的认证用户名一致**，即与本表下面被认证方设备上配置的第 3 步和第 4 步配置的用户名和密码一致。命令中的参数说明参见上节表 4-12 中认证方的第 6 步
7	**local-user** *user-name* **service-type ppp** 例如：[Huawei-aaa] **local-user** winda **service-type ppp**	配置参数 *user-name* 指定的本地用户（**要与上一步配置的用户名一致**）使用的服务类型为 PPP。其他说明参见上节表 4-12 中认证方设备上配置的第 7 步
认证方没有配置用户名时的被认证方配置		
3	**ppp chap user** *username* 例如：[Huawei-Serial1/0/0]**ppp chap user** winda	设置 CHAP 认证的用户名，是指被认证方向认证方发送的用户名（用于认证方对被认证方的认证，**不需要在被认证方本地创建**），在认证方上为被认证方配置的本地用户的用户名必须与此处配置的一致，即与本表中认证方设备配置的第 6 步通过 **local-user** 命令创建的用户名一致。其他说明参见本节表 4-13 中认证方设备配置的第 4 步

（续表）

步骤	命令	说明
4	**ppp chap password** { **cipher** | **simple** } *password* 例如：[Huawei-Serial1/0/0] **ppp chap password cipher** huawei	配置 CHAP 验证的密码，一定要与本表中认证方设备配置的第 6 步通过 **local-user** 命令创建的用户密码一致。命令中的参数和选项说明参见上节表 4-12 中被认证方设备配置的第 3 步 缺省情况下，未配置 CHAP 验证的密码，可用 **undo ppp chap password** 命令删除配置的密码

4.6.5 配置 PPP 协商参数

在设备上还可以有选择地配置一些用于 PPP 协商的参数，具体包括以下可选配置任务。

1. 协商超时时间间隔

在 PPP 协商过程中，如果在某个时间间隔内没有收到对端的应答报文，则 PPP 会重发前一次发送的报文，这个时间间隔称为“超时时间间隔”。但这个时间间隔设置过大，会降低链路传输效率；设置过小又将提高报文重发率，增加链路负担，需根据实际情况调整其缺省配置。

2. 协商轮询时间间隔

“轮询时间间隔”是指接口发送 keepalive（保持活跃）报文的周期。keepalive 报文用于链路状态监测维护，接口如果在 5 个 keepalive 周期之后仍然无法收到对端的 keepalive 报文，它就会认为链路发生故障。

在低速链路上，超大报文可能会需要很长的时间才能传送完毕，这样就会延迟 keepalive 报文的发送与接收。而接口如果在 5 个 keepalive 周期之后仍然无法收到对端的 keepalive 报文，它就会认为链路发生故障而自动关闭。为了避免这种情况发生，要根据实际情况调整其缺省配置。

3. 协商 DNS 服务器地址

设备在进行 PPP 地址协商的过程中可以进行 DNS 地址协商，此时设备既可以配置为接收对端分配的 DNS 地址，也可以配置为向对方提供 DNS 地址。

当设备通过 PPP 连接运营商的接入服务器时，设备应配置为被动接收或主动请求对端指定 DNS 地址，这样设备就可以使用接入服务器分配的 DNS 来解析域名。当 PC 与设备通过 PPP 相连时（通常为 PC 拨号连接设备），设备可以为 PC 指定 DNS 地址，这样 PC 就可以访问 Internet。但路由器不能同时配置成既为对端指定 DNS 服务器地址，又接收对端为其指定的 DNS 服务器地址。

以上三项配置任务的具体配置步骤如表 4-15 所示。

表 4-15　PPP 协商参数配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	进入接口视图，其他说明参见上节表 4-12 中的第 2 步

（续表）

<table>
<tr><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td>3</td><td>ppp timer negotiate seconds
例如：[Huawei-Serial1/0/0] ppp timer negotiate 5</td><td colspan="2">配置 PPP 协商超时时间间隔。参数 seconds 用来指定 PPP 协商超时时间间隔，取值范围为 1～10 整数秒
缺省情况下，PPP 协商超时时间间隔为 3 s，可用 undo ppp timer negotiate 命令恢复为缺省值</td></tr>
<tr><td>4</td><td>timer hold seconds
例如：[Huawei-Serial1/0/0] timer hold 60</td><td colspan="2">配置轮询时间间隔。参数 seconds 用来指定接口轮询时间间隔，取值范围为（1～32 767 整数秒。如果将轮询时间间隔配置为 0 s，则表示不发送 keepalive 报文
缺省情况下，轮询时间间隔为 10 s，可用 undo timer hold 命令恢复为缺省情况</td></tr>
<tr><td rowspan="3">5</td><td>ppp ipcp dns request
例如：[Huawei-Serial1/0/0]ppp ipcp dns request</td><td rowspan="2">（二选一）配置路由器接收对端分配的 DNS 服务器地址</td><td>配置设备主动向对端请求 DNS 服务器的 IP 地址
【说明】当设备通过 PPP 协议与其他设备相连时，若设备需要通过域名直接访问 Internet，则需要对端设备为其分配 DNS 服务器地址
缺省情况下，设备不会主动向对端请求 DNS 服务器地址，可用 undo ppp ipcp dns request 命令恢复为缺省情况</td></tr>
<tr><td>ppp ipcp dns admit-any
例如：[Huawei-Serial1/0/0]ppp ipcp dns admit-any</td><td>配置路由器被动地接收对端指定的 DNS 服务器地址
【说明】当设备通过 PPP 协议与其他设备相连时，若设备需要通过域名直接访问 Internet，则需要对端设备为其分配 DNS 服务器地址
缺省情况下，路由器不会被动地接收对端设备指定的 DNS 服务器的 IP 地址，可用 undo ppp ipcp dns admit-any 命令恢复为缺省情况</td></tr>
<tr><td>ppp ipcp dns primary-dns-address [secondary-dns-address]
例如：[Huawei-Serial1/0/0] ppp ipcp dns 10.10.10.10 10.10.10.11</td><td colspan="2">（二选一）配置设备为对端设备指定 DNS 服务器的 IP 地址。命令中的参数说明如下
● primary-dns-address：指定为对端提供的主 DNS 服务器的 IP 地址
● secondary-dns-address：可选参数，指定为对端提供的从 DNS 服务器的 IP 地址
【说明】当主机与设备通过 PPP 协议相连时，主机若想通过域名直接访问 Internet，则需要设备为主机指定 DNS 服务器地址
缺省情况下，设备不为对端设备指定 DNS 服务器的 IP 地址，可用 undo ppp ipcp dns primary-dns-address [secondary-dns-address] 命令禁止设备为对端设备指定 DNS 服务器的 IP 地址</td></tr>
</table>

4.6.6 PPP 管理

配置好 PPP 后，可以通过以下 **display** 命令查看 PPP 配置信息，验证配置结果，也

可以通过以下 **reset** 用户视图命令清除对应接口中的 PPP 压缩统计信息。

① **display this**：在对应接口视图下查看对应接口下配置 PPP 认证信息。

② **display local-user**：查看本地用户的配置情况。

③ **reset ppp compression iphc** [**interface** *interface-type interface-number*]：清除 IPHC 压缩统计信息。

④ **reset ppp compression stac-lzs** [**interface** *interface-type interface-number*]：清除 STAC-LZS 压缩统计信息。

4.6.7 PAP 单向认证配置示例

本示例的基本网络结构如图 4-13 所示，RouterA 的 Serial1/0/0 和 RouterB 的 Serial1/0/0 相连。用户希望 RouterA 对 RouterB 进行简单的认证，而 RouterB 不需要对 RouterA 进行认证。



图 4-13 PPP PAP 认证示例基本网络结构

很显然，根据本示例的要求，采用 PPP PAP 认证方式最简单。此时 RouterA 作为 PAP 认证的认证方，RouterB 作为 PAP 认证的被认证方。现仅以 AAA 本地认证方案为例进行介绍，具体的配置步骤如下。

1. 认证方 RouterA 上的配置

① 配置接口 Serial1/0/0 的 IP 地址及封装的链路层协议为 PPP。因为本示例中明确指定了双方接口的 IP 地址，所以可直接为双方配置 IP 地址，不采用 IP 地址协商方式。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol ppp
[RouterA-Serial1/0/0] ip address 10.10.10.9 30
```

② 配置 PPP 认证方式为 PAP、认证域名为 system。

```
[RouterA-Serial1/0/0] ppp authentication-mode pap domain system
[RouterA-Serial1/0/0] quit
```

③ 配置本地用户账户和域。因为要对被认证方进行认证，需要在本地创建用于认证的用户名和密码。此处仅以 AAA 中的本地认证方案为例进行介绍（有关 AAA 认证的其他方式配置具体参见配套图书《**华为交换机学习指南**》第 17 章）。

```
[RouterA] aaa
[RouterA-aaa] authentication-scheme system_a                   !---创建名为 system_a 的 AAA 认证方案
[RouterA-aaa-authen-system_a] authentication-mode local         !---指定以上认证方案采用本地认证方式
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system                                     !---创建名为 system 的域
[RouterA-aaa-domain-system] authentication-scheme system_a      !---将 system 域与 system_a 认证方案关联
[RouterA-aaa-domain-system] quit
[RouterA-aaa] local-user user1@system password cipher huawei123
[RouterA-aaa] local-user user1@system service-type ppp
[RouterA-aaa] quit
```

④ 重启接口，保证配置生效。

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] shutdown
[RouterA-Serial1/0/0] undo shutdown
```

2. 被认证方 RouterB 上的配置

① 配置接口 Serial1/0/0 的 IP 地址及封装的链路层协议为 PPP。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol ppp
[RouterB-Serial1/0/0] ip address 10.10.10.10 30
```

② 配置向认证方 RouterA 发送 PAP 认证的 PAP 用户名和密码。

```
[RouterB-Serial1/0/0] ppp pap local-user user1@system password simple huawei123
```

③ 重启接口，保证配置生效。

```
[RouterB-Serial1/0/0] shutdown
[RouterB-Serial1/0/0] undo shutdown
```

配置好后执行 **display interface serial** 1/0/0 命令查看接口的配置信息，验证配置结果。从中可以看出接口的物理层和链路层的状态都是 **Up**，并且 PPP 的 LCP 和 IPCP 都是 **opened** 状态（参见输出信息中粗体部分），说明链路的 PPP 协商已经成功，并且 RouterA 和 RouterB 可以互相 Ping 通对方。

```
[RouterB] display interface serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-03-25 11:35:10
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Internet Address is 10.10.10.9/30
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time     : 2011-03-25 11:35:10
Last physical down time : 2011-03-25 11:35:01
<省略>
```

4.6.8 PAP 双向认证配置示例

本示例的基本网络结构参见上节的图 4-13，此处不同的只是用户既希望 RouterA 对 RouterB 进行简单的 PAP 认证，也希望 RouterB 对 RouterA 进行认证。

根据本示例的双向 PAP 认证要求，可以得知需要配置 RouterA 既作为 PAP 认证的认证方也作为 PAP 认证的被认证方，同时 RouterB 既作为 PAP 认证的认证方也作为 PAP 认证的被认证方。

根据 4.6.3 小节介绍的配置方法可以很容易得出本示例的如下具体配置步骤（在此也仅以 AAA 中的本地认证方案为例进行介绍）。

1. RouterA 上的配置

① 配置接口 Serial1/0/0 的 IP 地址及封装的链路层协议为 PPP。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol ppp
[RouterA-Serial1/0/0] ip address 10.10.10.9 30
```

② 配置 PPP 认证方式为 PAP、认证域名为 system。

```
[RouterA-Serial1/0/0] ppp authentication-mode pap domain system
[RouterA-Serial1/0/0] quit
```

③ 配置本地用户及域。此处的用户名要与 RouterB 发送的 PAP 认证用户名和密码一致。

```
[RouterA] aaa
[RouterA-aaa] authentication-scheme system_a
[RouterA-aaa-authen-system_a] authentication-mode local
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme system_a
[RouterA-aaa-domain-system] quit
[RouterA-aaa] local-user user1@system password cipher huawei1
[RouterA-aaa] local-user user1@system service-type ppp
[RouterA-aaa] quit
```

④ 配置本地向 RouterB 发送的 PAP 认证用户名和密码，并重启接口，使配置生效。

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] ppp pap local-user user2@system password simple huawei2
[RouterA-Serial1/0/0] shutdown
[RouterA-Serial1/0/0] undo shutdown
```

2. RouterB 上的配置

① 配置接口 Serial1/0/0 的 IP 地址及封装的链路层协议为 PPP。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol ppp
[RouterB-Serial1/0/0] ip address 10.10.10.10 30
```

② 配置 PPP 认证方式为 PAP，认证域为 system。

```
[RouterB-Serial1/0/0] ppp authentication-mode pap domain system
[RouterB-Serial1/0/0] quit
```

③ 配置本地用户及域。此处的用户名要与 RouterA 发送的 PAP 认证用户名和密码一致。

```
[RouterB] aaa
[RouterB-aaa] authentication-scheme system_a
[RouterB-aaa-authen-system_a] authentication-mode local
[RouterB-aaa-authen-system_a] quit
[RouterB-aaa] domain system
[RouterB-aaa-domain-system] authentication-scheme system_a
[RouterB-aaa-domain-system] quit
[RouterB-aaa] local-user user2@system password cipher huawei2
[RouterB-aaa] local-user user2@system service-type ppp
[RouterB-aaa] quit
```

④ 配置本地向 RouterA 发送 PAP 认证用户名和密码，并重启接口，使配置生效。

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] ppp pap local-user user1@system password simple huawei1
[RouterB-Serial1/0/0] shutdown
[RouterB-Serial1/0/0] undo shutdown
```

可以用上节介绍的同样方法通过 **display interface serial** 1/0/0 命令查看接口上的 PPP 认证配置，以验证配置结果，具体输出示例略。

4.6.9 CHAP 单向认证配置示例

本示例的基本网络结构参见 4.6.7 小节的图 4-13，此处不同的只是用户希望 RouterA

对 RouterB 进行可靠的 CHAP 认证，而 RouterB 不需要对 RouterA 进行认证。此时，仅需要配置 RouterA 作为 CHAP 认证的认证方，RouterB 作为 CHAP 认证的被认证方。

为了更加安全可靠，本示例采用了认证方配置了用户名的情形，根据 4.6.4 小节表 4-13 介绍的配置方法可以很容易得出本示例的如下具体配置步骤（在此也仅以 AAA 中的本地认证方案为例进行介绍）。

1. 认证方 RouterA 上的配置

① 配置接口 Serial1/0/0 的 IP 地址及封装的链路层协议为 PPP。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol ppp
[RouterA-Serial1/0/0] ip address 10.10.10.9 30
```

② 配置 PPP 认证方式为 CHAP，用于被认证方 RouterB 进行认证方验证的用户名为 user1@system、认证域为 system。

```
[RouterA-Serial1/0/0] ppp authentication-mode chap domain system
[RouterA-Serial1/0/0] ppp chap user user1@system
[RouterA-Serial1/0/0] quit
```

③ 配置本地用户及域。本地用户是用来对被认证方 RouterB 进行认证的。

```
[RouterA] aaa
[RouterA-aaa] authentication-scheme system_a
[RouterA-aaa-authen-system_a] authentication-mode local
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme system_a
[RouterA-aaa-domain-system] quit
[RouterA-aaa] local-user user2@system password cipher huawei123
[RouterA-aaa] local-user user2@system service-type ppp
[RouterA-aaa] quit
```

④ 重启接口，保证配置生效。

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] shutdown
[RouterA-Serial1/0/0] undo shutdown
```

2. 被认证方 RouterB 上的配置

① 配置接口 Serial1/0/0 的 IP 地址及封装的链路层协议为 PPP。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol ppp
[RouterB-Serial1/0/0] ip address 10.10.10.10 30
```

② 配置本地向认证方 RouterA 发送的 CHAP 认证用户名。这个用户名一定要与在认证方 RouterA 上创建的本地用户名一致。

```
[RouterB-Serial1/0/0] ppp chap user user2@system
```

③ 重启接口，保证配置生效。

```
[RouterB-Serial1/0/0] shutdown
[RouterB-Serial1/0/0] undo shutdown
```

配置好后，同样可以通过 **display interface serial** 1/0/0 命令查看接口的配置信息，验证配置结果。具体输出示例略。

4.7 MP 配置与管理

MP（MultiLink PPP）是将多个 PPP 链路捆绑使用的技术，可以满足增加整个通信链路的带宽、增强可靠性（因为捆绑的多条链路之间具有冗余、备份功能）的需求。MP 捆绑的是物理 PPP 链路，包括 Serial 接口、Async 接口、CPOS 接口、ISDN BRI 接口、E1-F 接口、CE1/PRI 接口、T1-F 接口、CT1/PRI 接口、虚拟模板接口、CPOS 接口、POS 接口。

4.7.1 MP 概述

当用户对带宽的要求较高时，单个的 PPP 链路无法提供足够的带宽，这时将多个 PPP 链路进行捆绑形成 MP 链路，旨在增加链路的带宽并增强链路可靠性。

如图 4-14 所示，RouterA 和 RouterB 之间存在三条直连 PPP 链路，可以通过创建 MP 逻辑接口，将三条 PPP 链路进行捆绑，可以提供速率更高、带宽更宽的链路，且其中一条链路发生故障时，其他链路可以正常通信。

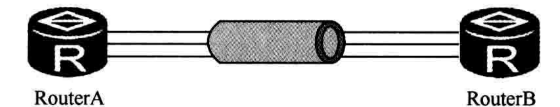


图 4-14 路由器通过 MP 链路通信示意图

MP 是通过 PPP 捆绑多条 PPP 链路来实现的，具体实现方式及应用场景如表 4-16 所示。

表 4-16 MP 实现方式分类及对比

分类	子分类	特点及应用场景	限制
采用虚拟模板（VT）接口实现 MP	将多条 PPP 链路直接绑定到 VT 上实现 MP	通过多条 PPP 链路和一个虚拟接口模板的直接绑定实现 MP，可以配置验证，也可以配置不验证 这种方法配置简单，但当采用不验证方式时安全性不高，因为可能被非法捆绑	同一个链路上这两种实现方式互斥
	按照 PPP 链路用户名查找 VT 实现 MP	系统可以根据验证通过的对端用户名找到绑定的虚拟接口模板，相同用户名绑定到一个虚拟接口模板。这种 MP 绑定方式一定要配置 PPP 验证，只有接口通过验证后，绑定才能生效 这种方法实现灵活，但配置复杂（因为每条 PPP 链路都要配置相同的 PPP 认证），一般用于灵活性要求较高的场合	
采用 MP-Group 实现 MP	将多条 PPP 链路加入 MP-Group 实现 MP	MP-Group 接口是 MP 的专用逻辑接口，不能支持其他应用，通过直接将多条 PPP 链路加入 MP-Group 实现 MP 这种方法快速高效、配置简单、容易理解，实际应用中多采用这种方法进行 PPP 绑定	-

说明 VT（Virtual-Template，虚拟模板）接口是用来在 PPP 链中需要承载其他链路层协议（如此处的 MP）时所采用的一种逻辑接口。另外，在 ATM 和 VPN 应用中也经常要用到 VT 接口，如 PPPoA 专线 ADSL 中就有 ATM 应用，需要使用 VT。在实际应用环境中，虚拟访问模板的创建和删除由系统自动完成，**但 VT 接口在链路**

层只支持 PPP，网络层只支持 IP（可直接配置 IP 地址，或者通过从对端协商获取 IP 地址）。

MP-Group 是一个专门用于 MP 的逻辑接口，通过建立接口和 MP-Group 的对应关系，将多个接口捆绑到一个 MP-Group 逻辑接口，实现 MP 捆绑。MP-Group 通常应用在具有动态带宽需求的场合。**但 MP-Group 接口在链路层只支持 PPP，网络层只支持 IP**（可直接配置 IP 地址，或者通过从对端协商获取 IP 地址）。

MP 建链过程与 PPP 建链过程类似，在 Dead 阶段与 Terminate 阶段与 PPP 一致，在其他阶段与 PPP 有一定区别，主要表现在以下几方面。

① 在 Establish 阶段，在 MP 中的 PPP 链路进行 LCP 协商时，除了协商一般 LCP 参数外，还要验证终端描述符是否一致，以及对端接口是否也工作在 MP 方式下。如果协商不一致，LCP 协商将不成功。

② 在 Authenticate 阶段，无论是 VT 接口还是 MP-Group 接口都不支持验证，只能在物理接口下进行验证配置。

③ 在 Network 阶段，是在 MP 链路上进行的 IPCP 协商，IPCP 协商通过后，MP 链路便可以正式使用，在上面传送 IP 报文了。

4.7.2 MP 主要特性

在 AR G3 系列路由器中，支持 MP 特性包括分片和最大捆绑数，但不支持跨板 MP。

1. MP 分片

在低速串行链路上实时交互式通信时，如 Telnet 和 VoIP，由于超大报文的发送而导致阻塞延迟。例如，当超大报文被调度而等待发送时，语音报文到达后可能需要等该超大报文被传输完毕后才能被调度，这会导致对端听到的话音断断续续。

交互式语音要求端到端的延迟小于等于 150 ms，一个 1 500 bytes 的报文需要花费 215 ms 穿过 56 kbit/s 的链路，这超过了人所能忍受的延迟限制。为了在低速链路上限制实时报文的延迟时间，需要一种方法将超大报文进行分片，将超大报文的分片和不需要分片的报文一起加入到队列。LFI（Link Fragmentation and Interleaving，链路分片和交叉）功能可将超大报文分割成小型报文（**缺省情况下，最小的分片为 500 个字节**），与其他不需要分片的高优先级报文一起发送，从而减少在速率较慢的链路上的延迟和抖动，保证了优先级高的报文优先传输。被分片的报文在到达目的地后再被重组。

图 4-15 描述了 LFI 的处理过程。超大报文和小的语音报文一起到达某个接口，将超大报文分割成小的分片，如果在接口配置了加权公平队列 WFQ（Weighted Fair Queueing），语音包与这些小的分片一起交叉放入 WFQ。

2. MP 最大捆绑数

通常情况下，如果需要限制 MP 链路的带宽，可以配置允许单一 MP 可以最大捆绑的 PPP 链路数。缺省情况下，一个 MP 最多捆绑 16 条 PPP 链路。

说明 MP 由多条 PPP 链路捆绑而成，可以在支持 PPP 的接口上应用。根据 4.7.1 小节表 4-16 所介绍的三种 MP 实现方式，下面三小节将分别介绍它们的具体配置方法，但在

配置 MP 之前，需确保每条被捆绑的 PPP 链路已建立成功。

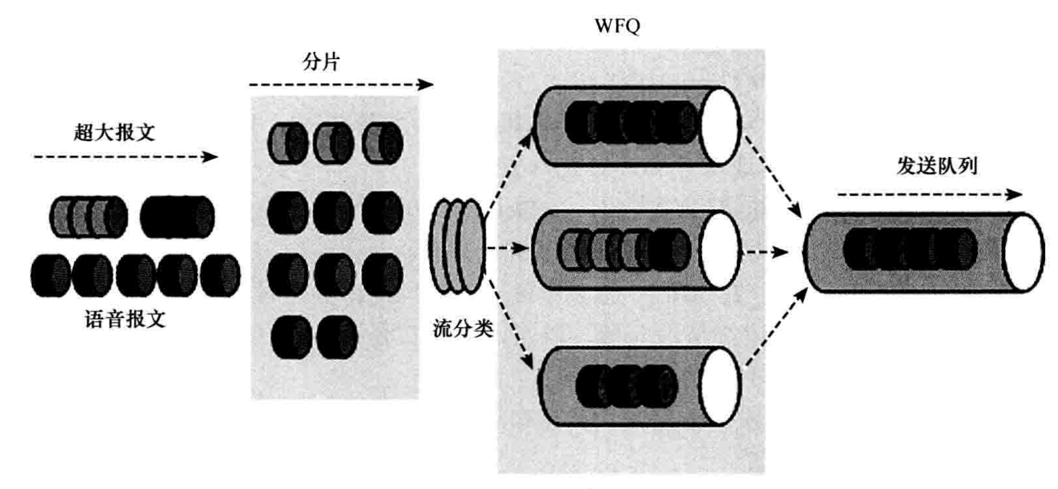


图 4-15　LFI 处理过程示意图

4.7.3　配置将 PPP 链路直接绑定到 VT 上实现 MP

设备通过多个接口和一个虚拟模板接口的直接绑定实现 MP。在这种 MP 实现方式下，可以配置 PPP 认证，也可以不配置 PPP 认证（**但认证均仅可在物理 PPP 接口上配置**）。配置 PPP 认证时，各 PPP 物理接口通过 PPP 认证后，绑定才能生效；不配置 PPP 认证时，当各 PPP 物理接口的 LCP 状态为 Up 后，绑定就生效。具体的配置步骤如表 4-17 所示。

注意　在采用 VT 进行 MP 直接绑定时，不能实现 VT 接口嵌套绑定，否则在一个 VT1 接口下绑定另一个 VT2 接口时，VT1 上的业务不能在 VT2 接口下生效。

表 4-17　　将 PPP 链路直接绑定到 VT 上实现 MP 的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface virtual-template** *vt-number* 例如：[Huawei] **interface virtual-template** 10	创建并进入指定的虚拟模板接口视图。参数用来指定创建的虚拟模板接口的编号，取值范围为 0～1 023 的整数
3	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-Virtual-Template10] **ip address** 10.1.1.1 24	（二选一）直接为 VT 接口配置 IP 地址。**不要再在各物理 PPP 链路接口配置 IP 地址**
	ip address ppp-negotiate 例如：[Huawei-Virtual-Template10] **ip address ppp-negotiate**	（二选一）配置本端 VT 接口接受 PPP 协商产生的由对端 VT 接口分配的 IP 地址。**不要再在各物理 PPP 链路接口配置 IP 地址**
4	**quit** 例如：[Huawei-Virtual-Template10] **quit**	退出 VT 接口视图，返回系统视图

（续表）

步骤	命令	说明
5	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	键入要绑定到 VT 中的物理接口，进入对应的物理接口视图
6	**ppp mp virtual-template** *vt-number* 例如：[Huawei-Serial1/0/0] **ppp mp virtual-template** 10	将以上物理接口绑定在指定 VT 上。这里的参数 *number* 取值要和步骤 2 中配置的 *number* 值一致
7	请根据需要配置认证或不配置，具体参见 4.6.3 小节和 4.6.4 小节	
8	重复步骤 5 至步骤 7，可以将多个接口和虚拟接口模板绑定，但对于需要绑定在一起的接口，必须采用同样的绑定方式	
9	为了使 PPP 重新协商，以保证所有物理接口成功绑定到 MP，配置完成后，请重启所有物理接口	

4.7.4 配置按照 PPP 链路用户名查找 VT 实现 MP

设备可以根据验证通过的对端用户名找到绑定的 VT 接口，使使用相同用户名认证的 PPP 链路被绑定到同一个 VT 接口上。这种 MP 绑定方式一定要配置 PPP 认证，只有接口通过 PPP 认证后，绑定才能生效。具体的配置步骤如表 4-18 所示。

表 4-18　按照 PPP 链路用户名查找 VT 实现 MP 的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface virtual-template** *vt-number* 例如：[Huawei] **interface virtual-template** 10	创建并进入指定的虚拟模板接口视图。参数用来指定创建的虚拟模板接口的编号，取值范围为 0～1 023 的整数
3	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-Virtual-Template10] **ip address** 10.1.1.1 24	（二选一）直接为 VT 接口配置 IP 地址。**不要再在各物理 PPP 链路接口配置 IP 地址**
	ip address ppp-negotiate 例如：[Huawei-Virtual-Template10] **ip address ppp-negotiate**	（二选一）配置本端 VT 接口接受 PPP 协商产生的由对端 VT 接口分配的 IP 地址。**不要再在各物理 PPP 链路接口配置 IP 地址**
4	**ppp mp binding-mode** { **authentication** | **descriptor** | **both** } 例如：[Huawei-Virtual-Template10] **ppp mp binding-mode authentication**	配置 MP 捆绑的条件。命令中的选项说明如下 ● **authentication**：多选一选项，指定根据对端用于 PPP 认证的用户名进行 PPP 捆绑 ● **descriptor**：多选一选项，指定根据对端设备的终端标识符进行 PPP 捆绑。此时要根据需要在对端设备上使用 **ppp mp endpoint** *endpoint-name* 命令配置终端描述符（1～20 个字符，不支持空格，**区分大小写**，当一个设备有多个 MP 时，可以配置多个终端描述符） ● **both**：多选一选项，指定同时根据对端用户名和终端标识符进行 PPP 捆绑 配置的 MP 捆绑条件需要和对端保持一致，否则会导致 MP 协商异常 缺省情况下，同时根据对端用户名和终端标识符进行 MP 捆绑，即捆绑模式为 **both**，可用 **undo ppp mp binding-mode** 命令恢复 PPP 捆绑条件为缺省条件

（续表）

步骤	命令	说明
5	**quit** 例如：[Huawei-Virtual-Template10] **quit**	退出 VT 接口视图，返回系统视图
6	**ppp mp user** *username* **bind virtual-template** *vt-number* 例如：[Huawei] **ppp mp user** winda **bind virtual-template** 10	配置对端用户和虚拟接口模板的对应关系。命令中的参数说明如下 ● *username*：指定用户名，即指定 PPP 链路进行 PAP 或 CHAP 认证时所接收到的对端用户名，1～64 字符，不支持空格，**区分大小写** ● *vt-number*：指定以上用户名要绑定的虚拟模板接口号，取值范围为 0～1 023 的整数. 这里的参数 *number* 取值要和步骤 2 中配置的 *number* 值一致
7	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	键入要绑定到 VT 中的物理接口，进入对应的物理接口视图
8	**ppp mp** 例如：[Huawei-Serial1/0/0] **ppp mp**	配置封装 PPP 的接口工作在 MP 方式 缺省情况下，接口工作在普通 PPP 方式，可用 **undo ppp mp** 命令恢复为缺省方式
9	在接口下配置 PPP 双向认证(可以是 PAP 认证或者 CHAP 认证)，具体参见 4.6.3 小节和 4.6.4 小节	
10	重复步骤 7 至步骤 9，可以将多个接口和虚拟接口模板绑定，但对于需要绑定在一起的接口，必须采用同样的绑定方式	
11	为了使 PPP 重新协商，以保证所有物理接口成功绑定到 MP，配置完成后，请重启所有物理接口	

4.7.5 配置将 PPP 链路加入 MP-Group 实现 MP

MP-Group 是一个专门用于 MP 的逻辑接口，通过建立接口和 MP-Group 的对应关系，将多个接口加入到一个 MP-Group 逻辑接口，实现 MP。而且这种方式实现更为简单，广泛被采用，具体配置步骤如表 4-19 所示。

表 4-19　　将 PPP 链路加入 MP-Group 实现 MP 的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface virtual-template** *vt-number* 例如：[Huawei] **interface virtual-template** 10	创建并进入指定的虚拟模板接口视图。参数 *vt-number* 用来指定创建的虚拟模板接口的编号，取值范围为 0～1 023 的整数
3	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-Virtual-Template10] **ip address** 10.1.1.1 24	（二选一）直接为 VT 接口配置 IP 地址。**不要再在各物理 PPP 链路接口配置 IP 地址**
	ip address ppp-negotiate 例如：[Huawei-Virtual-Template10] **ip address ppp-negotiate**	（二选一）配置本端 VT 接口接受 PPP 协商产生的由对端 VT 接口分配的 IP 地址。**不要再在各物理 PPP 链路接口配置 IP 地址**

（续表）

步骤	命令	说明
4	**quit** 例如：[Huawei-Virtual-Template10] **quit**	退出 VT 接口视图，返回系统视图
5	**interface** *interface-type interface-number* 例如：[Huawei] **interface serial** 1/0/0	键入要绑定到 VT 中的物理接口，进入对应的物理接口视图
6	**ppp mp mp-group** *number* 例如：[Huawei-Serial1/0/0] **ppp mp mp-group** 10	将物理接口加入指定的 MP-Group，使该接口工作在 MP 方式。**这里的参数 *number* 取值要和步骤 2 中配置的 *vt-number* 值一致** 缺省情况下，接口工作在普通 PPP 方式下，可用 **undo ppp mp** 命令恢复缺省值
7	请根据需要配置认证或不配置，具体参见 4.6.3 小节和 4.6.4 小节	
8	重复步骤 5 至步骤 7，可以将多个接口和虚拟接口模板绑定，但对于需要绑定在一起的接口，必须采用同样的绑定方式	
9	为了使 PPP 重新协商，以保证所有物理接口成功绑定到 MP，配置完成后，请重启所有物理接口	

4.7.6 配置 MP 分片和捆绑数

MP 的分片功能可以通过两种方法来实现：一是直接在 MP 中要使用的 VT 接口或者 MP-Group 接口下手动配置允许的最小分片大小；二是通过 VT 接口或者 MP-Group 接口下的 LFI 功能，使系统自动对报文进行分片。而 MP 捆绑数的配置就是配置一个 MP 中允许捆绑的最大 PPP 链路数。这两项配置任务都很简单，具体配置步骤如表 4-20 所示。

表 4-20　MP 分片和捆绑数的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface virtual-template** *vt-number* 例如：[Huawei] **interface virtual-template** 10	创建并进入指定的虚拟模板接口视图。参数用来指定创建的虚拟模板接口的编号，取值范围为 0～1 023 的整数
3	**ppp mp min-fragment** *size* 例如：[Huawei-Virtual-Template10] **ppp mp min-fragment** 800	（二选一）配置多链路捆绑中对 MP 出报文进行分片的最小报文长度。参数 *size* 用来指定 MP 出报文进行分片的最小报文长度。当 MP 出报文长度小于这个值则不进行分片，大于等于这个值则开始分片，取值范围为 128～1 500 个字节。一般情况下，分片的最小报文长度不需要配置，推荐使用缺省值 此命令在 LFI 功能未使能时生效 缺省情况下，对 MP 出报文进行分片的最小报文长度为 500 字节，可用 **undo ppp mp min-fragment** 命令恢复为缺省值

（续表）

步骤	命令	说明
3	**ppp mp lfi** 例如：[Huawei-Virtual-Template10] **ppp mp lfi**	（二选一）在以上接口上使能链路分片与交叉 LFI 功能 【说明】使能 LFI 功能后，分片的大小=（分片最大时延*接口的承诺信息速率）/8，单位为字节。其中，分片最大时延由 **ppp mp lfi delay-per-frag** *max-delay* 命令配置，接口的承诺信息速率由 **qos gts** cir *cir-value* [**cbs** *cbs-value*] 命令配置，但不受上面介绍的 **ppp mp min-fragment** *size* 命令配置的分片大小制约。如果接口的承诺信息速率未配置，则分片的大小固定为 500 字节 缺省情况下，接口上未使能 LFI 功能，可用 **undo ppp mp lfi** 命令去使能接口的 LFI 功能
4	**ppp mp max-bind** *max-bind-number* 例如：[Huawei-Virtual-Template10] **ppp mp max-bind** 10	在以上接口上配置 MP 最大捆绑链路数。参数 *max-bind-number* 用来指定当前 MP 可以捆绑的最大的 PPP 链路数，取值范围为 1～32 的整数 缺省情况下，MP 最大捆绑链路数的值为 16，可用 **undo ppp mp max-bind** 命令恢复为缺省值。仅在需要绑定后的接口带宽不能超过指定带宽时才要配置 MP 最大捆绑链路数
5	**shutdown** 和 **undo shutdown** 或 **restart** 例如：[Huawei-Virtual-Template10] **restart**	重启以上 VT 接口或者 MP-Group 接口，使配置生效

4.7.7 MP 管理

配置好 PPP 协议后，可以通过以下 **display** 任意视图命令查看 PPP 配置信息，验证配置结果。

① **display ppp mp** [**interface** *interface-type interface-number*]：查看 MP 的捆绑信息及捆绑链路的统计信息。

② **display interface virtual-template** [*vt-number*]：查看指定虚拟模板接口的状态信息。

③ **display interface mp-group** [*number*]：查看指定 MP-Group 接口的状态信息。

4.7.8 将 PPP 链路直接绑定到 VT 上实现 MP 的配置示例

本示例的基本网络结构如图 4-16 所示，路由器 RouterA 和 RouterB 的两对串口分别相连。现用户希望采用配置简单、安全性不需要很高的方法增加传输带宽，以保证数据的传输。

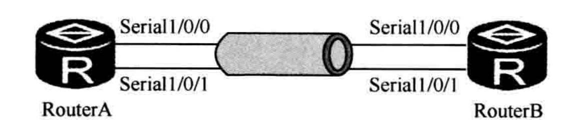


图 4-16 将 PPP 链路直接绑定到 VT 上实现 MP 配置示例的基本网络结构

本示例中用户要求配置简单，可以使用将PPP链路直接绑定到VT上的方式来实现MP，同时用户对安全性要求又不高，故可无需配置每条PPP链路的用户认证。因为RouterA和RouterB的配置是对称的，基本一样（不同的只是IP地址），故在此仅以RouterA上的配置为例进行介绍。具体配置步骤如下。

① 创建并配置虚拟模板接口VT1，然后根据图示为VT1配置IP地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ip address 10.10.10.9 30
[RouterA-Virtual-Template1] quit
```

② 配置物理接口Serial1/0/0、Serial1/0/1和前面创建的VT1直接绑定，使物理接口工作在MP方式。

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] ppp mp virtual-template 1
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 1/0/1
[RouterA-Serial1/0/1] ppp mp virtual-template 1
[RouterA-Serial1/0/1] quit
```

RouterB上的配置与以上RouterA上的配置基本一样，参见即可（只是它的VT1接口IP地址不一样，为10.10.10.10/30）。

配置好后，可使用**display ppp mp**命令查看绑定效果。下面是在RouterA上输出的结果。从输出显示的信息可以看到：**Bundle 10cd6d925ac6，**表示MP是通过虚拟接口模板直接绑定的，其中**10cd6d925ac6**是对端设备的终端描述符；从"The bundled sub channels are:"下面的列表可以看出，当前MP包含两个子链路，分别是Serial1/0/0和Serial1/0/1。

```
[RouterA] display ppp mp
Template is Virtual-Template1
 Bundle 10cd6d925ac6, 2 members, slot 0, Master link is Virtual-Template1:0
  0 lost fragments, 0 reordered, 0 unassigned,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial1/0/1
```

4.7.9 按照PPP链路用户名查找VT实现MP的配置示例

本示例的基本网络结构仍参见上节的图4-16，不同的只是现用户希望维护方便，需要根据PPP链路的用户名灵活地增加或减少传输带宽，且对安全性要求较高。

根据本示例用户希望维护方便和较高安全性的要求，可以选择使用按照PPP链路用户名查找VT实现MP的方式，并在每条PPP链路上配置CHAP双向认证。具体配置步骤如下。

1. RouterA上的配置

① 创建并配置虚拟模板接口VT1，并指定采用根据对端用户名进行PPP捆绑，为VT1接口配置IP地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
```

```
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ip address 10.10.10.9 30
[RouterA-Virtual-Template1] ppp mp binding-mode authentication   !---指定根据对端用户名进行 PPP 捆绑
[RouterA-Virtual-Template1] quit
```

② 配置 VT1 要绑定的对端用户名。

```
[RouterA] ppp mp user userb@system bind virtual-template 1
```

③ 配置物理接口 Serial1/0/0、Serial1/0/1 工作在 MP 方式，并采用 CHAP 认证，配置设备作为认证方时需要配置的本地用户以及作为被认证方时需要的 CHAP 认证用户名和密码。

```
[RouterA] aaa
[RouterA-aaa] local-user userb@system password cipher userb123  !---创建用于对对端进行认证的用户名和密码
[RouterA-aaa] local-user userb@system service-type ppp          !---指定用户 userb@system 使用 PPP 服务
[RouterA-aaa] authentication-scheme system_a                    ! ---创建一个名为 system_a 的 AAA 认证方案
[RouterA-aaa-authen-system_a] authentication-mode local         !---指定 system_a AAA 认证方案采用本地认证方式
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system                                     !---创建名为 system 的域
[RouterA-aaa-domain-system] authentication-scheme system_a !---将 system 域与 system_a 认证方案关联
[RouterA-aaa-domain-system] quit
[RouterA-aaa] quit
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] ppp authentication-mode chap domain system   !---指定接口采用 CHAP 认证，域名为 system
[RouterA-Serial1/0/0] ppp chap user usera@system               !---指定向对端发送用于CHAP认证的用户名为usera@system
[RouterA-Serial1/0/0] ppp chap password simple usera            !---指定以上 usera@system 用户的密码为 usera
[RouterA-Serial1/0/0] ppp mp                                    !---指定以上接口工作 MP 方式
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 1/0/1
[RouterA-Serial1/0/1] ppp authentication-mode chap domain system
[RouterA-Serial1/0/1] ppp chap user usera@system
[RouterA-Serial1/0/1] ppp chap password simple usera
[RouterA-Serial1/0/1] ppp mp
[RouterA-Serial1/0/1] quit
```

④ 重启 Serial1/0/0、Serial1/0/1 接口，使 MP 配置生效。

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] shutdown
[RouterA-Serial1/0/0] undo shutdown
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 1/0/1
[RouterA-Serial1/0/1] shutdown
[RouterA-Serial1/0/1] undo shutdown
[RouterA-Serial1/0/1] quit
```

2. RouterB 上的配置

① 创建并配置虚拟模板接口 VT1，并指定采用根据对端用户名进行 PPP 捆绑，为 VT1 接口配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ip address 10.10.10.10 30
[RouterB-Virtual-Template1] ppp mp binding-mode authentication
[RouterB-Virtual-Template1] quit
```

② 配置对端用户名和 VT1 绑定。

```
[RouterB] ppp mp user usera@system bind virtual-template 1
```

③ 配置物理接口 Serial1/0/0、Serial1/0/1 工作在 MP 方式及物理接口采用 CHAP 认证，配置设备作为认证方时需要配置的本地用户以及作为被认证方时需要的 CHAP 认证用户名和密码。

```
[RouterB] aaa
[RouterB-aaa] local-user usera@system password cipher usera123
[RouterB-aaa] local-user usera@system service-type ppp
[RouterB-aaa] authentication-scheme system_b
[RouterB-aaa-authen-system_b] authentication-mode local
[RouterB-aaa-authen-system_b] quit
[RouterB-aaa] domain system
[RouterB-aaa-domain-system] authentication-scheme system_b
[RouterB-aaa-domain-system] quit
[RouterB-aaa] quit
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] ppp authentication-mode chap domain system
[RouterB-Serial1/0/0] ppp chap user userb@system
[RouterB-Serial1/0/0] ppp chap password simple userb
[RouterB-Serial1/0/0] ppp mp
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 1/0/1
[RouterB-Serial1/0/1] ppp authentication-mode chap domain system
[RouterB-Serial1/0/1] ppp chap user userb@system
[RouterB-Serial1/0/1] ppp chap password simple userb
[RouterB-Serial1/0/1] ppp mp
[RouterB-Serial1/0/1] quit
```

④ 重启 Serial1/0/0、Serial1/0/1 接口，使 MP 配置生效。

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] shutdown
[RouterB-Serial1/0/0] undo shutdown
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 1/0/1
[RouterB-Serial1/0/1] shutdown
[RouterB-Serial1/0/1] undo shutdown
[RouterB-Serial1/0/1] quit
```

配置好后，可在 RouterA 和 RouterB 上分别执行 **display ppp mp** 命令，检查配置结果，查看绑定效果。以下是在 RouterA 上的输出结果。

```
[RouterA] display ppp mp
Template is Virtual-Template1
 Bundle userb@system, 2 members, slot 0, Master link is Virtual-Template1:0
  0 lost fragments, 0 reordered, 0 unassigned,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial1/0/1
```

根据显示信息可以看出：**Bundle userb@system** 表示 MP 是通过用户名验证绑定虚拟接口模板生成的，包含 Serial1/0/0 和 Serial1/0/1 两个成员等信息。

4.7.10 将 PPP 链路加入 MP-Group 实现 MP 的配置示例

本示例的基本网络结构仍参见上节的图 4-16，不同的只是用户希望采用配置快速高

效、简单且安全性较高的方法增加传输带宽，以保证数据的传输。根据用户的要求，可以将 PPP 链路加入 MP-Group 实现 MP，并对物理接口采用 CHAP 双向认证。具体配置步骤如下。

1. RouterA 上的配置

① 创建并配置 MP-Group 接口，并为 MP-Group 接口配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface mp-group 0/0/1
[RouterA-Mp-group0/0/1] ip address 100.10.10.9 30
[RouterA-Mp-group0/0/1] quit
```

② 把物理接口 Serial1/0/0、Serial1/0/1 加入 MP-Group，并配置接口采用 CHAP 认证，配置设备作为认证方时需要配置的本地用户以及作为被认证方时需要的 CHAP 认证用户名和密码。

```
[RouterA] aaa
[RouterA-aaa] local-user userb password cipher userb123
[RouterA-aaa] local-user userb service-type ppp
[RouterA-aaa] authentication-scheme system_a
[RouterA-aaa-authen-system_a] authentication-mode local
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme system_a
[RouterA-aaa-domain-system] quit
[RouterA-aaa] quit
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] ppp authentication-mode chap domain system
[RouterA-Serial1/0/0] ppp chap user usera
[RouterA-Serial1/0/0] ppp chap password simple usera
[RouterA-Serial1/0/0] ppp mp mp-group 0/0/1
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 1/0/1
[RouterA-Serial1/0/1] ppp authentication-mode chap domain system
[RouterA-Serial1/0/1] ppp chap user usera
[RouterA-Serial1/0/1] ppp chap password simple usera
[RouterA-Serial1/0/1] ppp mp mp-group 0/0/1
[RouterA-Serial1/0/1] quit
```

③ 重启 RouterA 上的 MP 成员接口 Serial1/0/0、Serial1/0/1。

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] restart
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 1/0/1
[RouterA-Serial1/0/1] restart
```

2. RouterB 上的配置

① 创建并配置 MP-Group 接口，并为 MP-Group 接口配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface mp-group 0/0/1
[RouterB-Mp-group0/0/1] ip address 100.10.10.10 30
[RouterB-Mp-group0/0/1] quit
```

② 将物理接口 Serial1/0/0、Serial1/0/1 加入 MP-Group，并配置接口采用 CHAP 认

证，配置设备作为认证方时需要配置的本地用户以及作为被认证方时需要的 CHAP 认证用户名和密码。

```
[RouterB] aaa
[RouterB-aaa] local-user usera password cipher usera123
[RouterB-aaa] local-user usera service-type ppp
[RouterB-aaa] authentication-scheme system_b
[RouterB-aaa-authen-system_b] authentication-mode local
[RouterB-aaa-authen-system_b] quit
[RouterB-aaa] domain system
[RouterB-aaa-domain-system] authentication-scheme system_b
[RouterB-aaa-domain-system] quit
[RouterB-aaa] quit
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] ppp authentication-mode chap domain system
[RouterB-Serial1/0/0] ppp chap user userb
[RouterB-Serial1/0/0] ppp chap password simple userb
[RouterB-Serial1/0/0] ppp mp mp-group 0/0/1
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 1/0/1
[RouterB-Serial1/0/1] ppp authentication-mode chap domain system
[RouterB-Serial1/0/1] ppp chap user userb
[RouterB-Serial1/0/1] ppp chap password simple userb
[RouterB-Serial1/0/1] ppp mp mp-group 0/0/1
[RouterB-Serial1/0/1] quit
```

③ 重启 RouterB 上的 MP 成员接口 Serial1/0/0、Serial1/0/1。

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] restart
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 1/0/1
[RouterB-Serial1/0/1] restart
```

配置好后同样可以使用 **display ppp mp** 命令检查配置结果，查看绑定效果。下面是在 RouterA 上执行的结果。从中可以看出 MP 子链路的物理状态和协议状态、子链路数及 MP 的成员等信息。

```
[RouterA] display ppp mp interface Mp-group 0/0/1
Mp-group is Mp-group0/0/1
 ==========Sublinks status begin======
 Serial1/0/0 physical UP,protocol UP
 Serial1/0/1 physical UP,protocol UP
 ==========Sublinks status end=======
 Bundle Multilink, 2 members, slot 0, Master link is Mp-group0/0/1
  0 lost fragments, 0 reordered, 0 unassigned,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial1/0/1
```

4.8 PPPoE 配置与管理

PPPoE（PPP over Ethernet，基于以太网的 PPP）是指在以太网链路上运行 PPP，在

ADSL、小区组网建设等应用中广泛采用。PPPoE 使用 Client/Server 模型，提供了在以太网网络中多台主机连接到远端的宽带接入 PPPoE 服务器上的一种标准。PPPoE 客户端向 PPPoE 服务器发起连接请求，两者之间会话协商通过后，PPPoE 服务器向 PPPoE 客户端提供接入控制、认证等功能。在 AR G3 系列路由器中，AR151、AR151W-P、AR151G-HSPA+7、AR201 和 AR201VW-P 仅支持 PPPoE 客户端，其他系列或机型均可同时支持 PPPoE 客户端和 PPPoE 服务器。

4.8.1 PPPoE 工作原理

PPPoE 组网结构采用 Client/Server 模型，PPPoE 客户端向 PPPoE 服务器发起连接请求，PPPoE 服务器为 PPPoE 客户端提供接入控制、认证等功能。PPPoE 会话建立流程可分为 3 个阶段，即 Discovery（发现）阶段、Session（会话）阶段和 Terminate（结束）阶段，如图 4-17 所示。下面对这三个阶段的工作流程分别进行介绍。

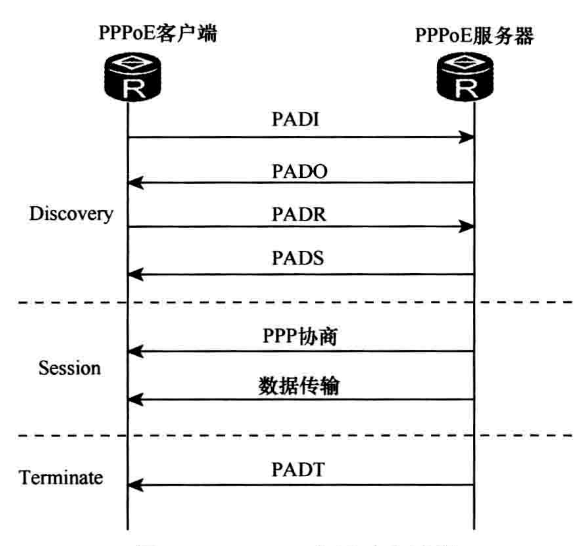


图 4-17 PPPoE 会话建立流程

1. Discovery 阶段

Discovery 阶段由以下 4 个过程组成。

① PPPoE 客户端广播发送一个 PADI（PPPoE Active Discovery Initial，PPPoE 激活发现初始化）报文，在此报文中包含 PPPoE 客户端想要得到的服务类型信息。

② 所有的 PPPoE 服务器在收到 PADI 报文之后，将其中请求的服务与自己能够提供的服务进行比较，如果可以提供，则单播回复一个 PADO（PPPoE Active Discovery Offer，PPPoE 激活发现提供）报文。

③ 根据网络的拓扑结构，PPPoE 客户端可能会收到多个 PPPoE 服务器发送的 PADO 报文，此时选择最先收到的 PADO 报文对应的 PPPoE 服务器作为自己的 PPPoE 服务器，并向该服务器单播发送一个 PADR（PPPoE Active Discovery Request，PPPoE 激活请求）报文。

④ PPPoE 服务器在收到 PADR 报文后，会产生一个唯一的会话 ID（Session ID），

用以标识和 PPPoE 客户端的这个会话，然后通过发送一个 PADS（PPPoE Active Discovery Session-confirmation，PPPoE 激活发现会话确认）报文把会话 ID 发送给 PPPoE 客户端，会话建立成功后便进入 PPPoE Session 阶段。

完成之后，通信双方都会知道 PPPoE 的 Session_ID 以及对方以太网地址，它们共同确定了唯一的 PPPoE 会话。

2. Session 阶段

PPPoE Discovery 阶段的工作为 PPPoE 客户端和 PPPoE 服务器之间建立了 Session（会话），之后 PPPoE 便进入 Session 阶段，Session 阶段可划分为两部分，一是 PPP 协商阶段，二是 PPP 报文传输阶段。

PPPoE Session 上的 PPP 协商和普通的 PPP 协商方式一致，分为 LCP、认证、NCP 三个阶段。

① LCP 阶段主要完成建立、配置和检测数据链路连接的任务。

② LCP 协商成功后，开始进行认证工作，认证协议类型由 LCP 协商结果（CHAP 或者 PAP）决定。

③ 认证成功后，PPP 进入 NCP 阶段。NCP 是一个协议族，用于配置不同的网络层协议，常用的是 IP 控制协议（IPCP），它负责配置用户的 IP 地址和 DNS 服务器地址等工作。

PPPoE Session 的 PPP 协商成功后，就可以承载 PPP 数据报文。

在 PPPoE Session 阶段所有的以太网数据包都是单播发送的。

3. Terminate 阶段

PPP 通信双方应该使用 PPP 自身来结束 PPPoE 会话，但在无法使用 PPP 结束会话时可以使用 PADT（PPPoE Active Discovery Terminate，PPPoE 激活发现终止）报文。

进入 PPPoE Session 阶段后，PPPoE 客户端和 PPPoE 服务器都可以通过发送 PADT 报文的方式结束 PPPoE 连接。PADT 数据包可以在会话建立以后的任意时刻单播发送。在发送或接收到 PADT 后，就不允许再使用该会话发送 PPP 流量了。

4.8.2　PPPoE 典型应用

根据 PPP 会话的起止点所在位置的不同，有两种组网结构。第一种部署方式是将企业中的路由器设备作为 PPPoE 客户端，与位于运营商中担当 PPPoE 服务器的路由器设备间建立 PPPoE 会话，如图 4-18 所示（如典型企业的 ADSL 互联网接入）。此时，所有内网主机的数据到达 PPPoE 客户端后，通过 PPP 会话传送出去，用户主机上不用安装 PPPoE 客户端拨号软件，一般是一个企业（公司）共用一个账号。

第二种部署方式是将路由器设备作为 PPPoE 服务器，在 Host 和运营商的路由器之间建立 PPPoE 会话，如图 4-19 所示。内网中的每台主机与担当 PPPoE 服务器的路由器建立一个 PPPoE 会话，典型应用如小区互联网接入。每台主机都是一个 PPPoE 客户端，安装 PPPoE 客户端拨号软件，单独使用一个账号，方便运营商对用户进行计费和控制。

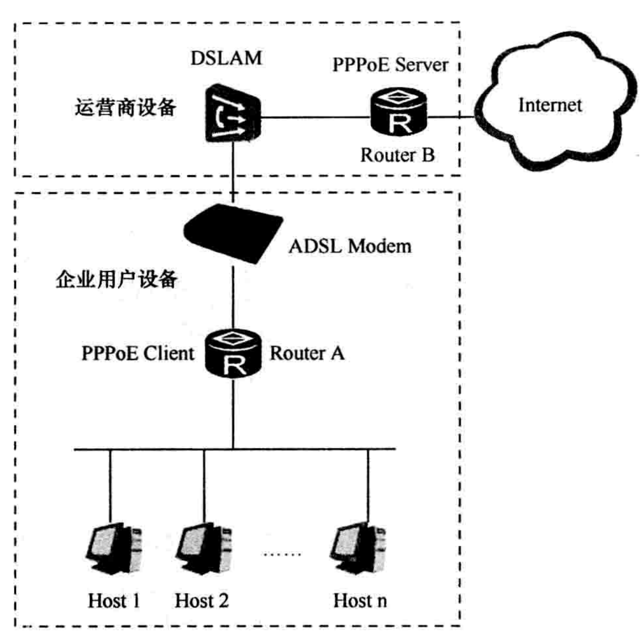


图 4-18 路由器作为 PPPoE 客户端的应用示例

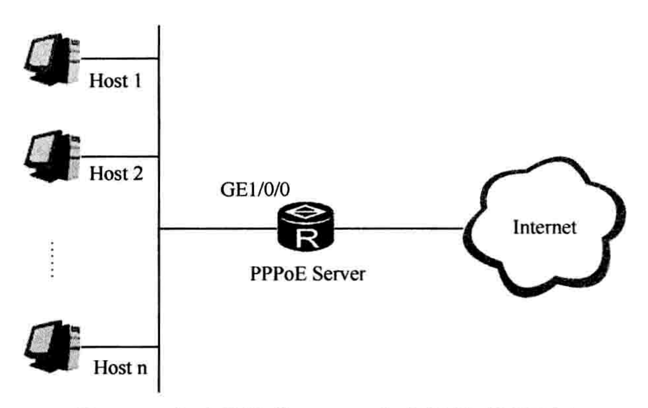


图 4-19 路由器作为 PPPoE 服务器的应用示例

4.8.3 配置设备作为 PPPoE 客户端

PPPoE 会话支持的接口有：以太网接口、PON 接口和 ATM 接口。当路由器作为 PPPoE 客户端时，可使同一个局域网中的所有主机共享一个 ADSL 账号进行拨号上网。主要包括以下四项配置任务。

1.（可选）配置 ADSL 接口

如果采用的是内置 ADSL Modem 功能，则要使用路由器上的 ADSL 接口（**是 ATM 接口**）连接 PPPoE 链路，这时就要配置 ADSL 接口。这方面主要是为 ADSL 接口选择所用 ADSL 标准以及选择打开或关闭比特交换开关、无缝速率自适应开关和格栅编码开关等特性。在配置这些特性前一定要先关闭 ADSL 接口，配置好后再打开 ADSL 接口，**具体配置方法参见本书 3.12 节**。

如果采用的是外置 ADSL Modem 连接方式，则不用进行本项配置任务，因为此时这些配置是在 ADSL Modem 上进行的。

2. 配置 Dialer 接口

因为在 AR G3 系列路由器中，无论采用哪种 ADSL 连接方式，ADSL PPPoE 拨号都是通过 DCC 控制的，所以都需要配置 DCC 参数。但又因为 ADSL 接口仅可工作于共享 DCC 方式，所以仅可在逻辑的 Dialer 接口上配置 DCC 参数，包括 Dialer 接口的 IP 地址分配（可以直接配置 IP 地址，也可配置采用协商方式从对端获取，拨号方式一般是采用协商方式）、PPP 协议封装，具体步骤参见 4.3.1 小节的表 4-2；配置 Dialer 接口属性，参见 4.3.4 小节表 4-6；使能共享 DCC 拨号等，具体配置步骤参见 4.4 节的表 4-9。

3. 在物理拨号接口上启用 PPPoE 客户端协议，建立 PPPoE 会话

PPPoE 会话支持的接口有以太网接口、PON 接口和 ATM 接口。

① 当设备通过以太网接口或 PON 接口连接 ADSL Modem 后再连入 Internet 的时候，需要在以太网接口或 PON 接口配置 PPPoE 会话。

② 当设备通过 ATM 接口连入 Internet 的时候，需要在虚拟以太网接口配置 PPPoE 会话。

PPPoE 会话有两种工作方式：永久在线方式和报文触发方式。

① 永久在线方式：当物理线路 Up 后，设备会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户删除 PPPoE 会话，否则此 PPPoE 会话将一直存在。

② 报文触发方式：当物理线路 Up 后，设备不会立即发起 PPPoE 呼叫，只有当有数据需要传送时，设备才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户的配置，设备会自动中止 PPPoE 会话。

4. （可选）配置 NAT，使内网用户 IP 地址转换成公网 IP 地址

当设备作为 PPPoE 客户端下行接局域网内用户时，因为局域网内用户使用的 IP 地址为私有地址，所以需要在设备上配置 NAT 将私网地址转换为公网地址，以使局域网内用户正常接入 Internet。**有关 NAT 方面的配置将在本书第 6 章介绍。**

下面仅介绍以上第 3 项配置任务。当设备通过以太网接口或 PON 接口连接外置 ADSL Modem 后再连入 Internet 时，在 ADSL 接口上启用 PPPoE 客户端协议的配置步骤如表 4-21 所示；当设备通过 ATM 接口直接连入 Internet 时，在 ADSL 接口上启用 PPPoE 客户端协议的配置步骤如表 4-22 所示。

表 4-21　通过以太网接口或 PON 接口连接外置 ADSL Modem 再连入 Internet 时的 PPPoE 配置

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface gigabitethernet** 1/0/0	键入 ADSL 接口（**采用内置 ADSL Modem 连接时**），或者以太网接口和 PON 接口（**采用外置 ADSL Modem 连接时**） 此处仅以采用以太网接口的外置连接方式为例进行介绍

（续表）

步骤	命令	说明
3	**pppoe-client dial-bundle-number** *number* [**on-demand**] [**no-hostuniq**] [**ppp-max-payload** *value*] 例如：[Huawei-GigabitEthernet1/0/0] **pppoe-client dial-bundle-number** 1	建立一个 PPPoE 会话，并指定 PPPoE 会话对应的 Dialer Bundle。命令中的参数和选项说明如下 ● *number*：指定与 PPPoE 会话相对应的 Dialer Bundle（拨号捆绑）编号，取值范围为 1～255 的整数，可以用来唯一标识一个 PPPoE 会话，也可以把它作为 PPPoE 会话的编号。一定要与在 Dialer 接口上配置的拨号捆绑号一致 ● **on-demand**：可选项，指定 PPPoE 客户端拨号方式为按需拨号，则需要在 Dialer 接口下使用 **dialer timer idle** *seconds* 命令配置闲置切断时间（取值范围为 0～65 535 的整数秒，缺省值为 120 s）。目前设备支持的按需拨号方式为报文触发方式。如果不选择此可选项，则 PPPoE 会话工作在永久在线方式 ● **no-hostuniq**：可选项，指定在 PPPoE 客户端发起的呼叫中不携带 Host-Uniq 字段。缺省情况下，PPPoE 客户端发起的呼叫中携带 Host-Uniq 字段。该字段用于与主机的某个唯一特定的请求联系起来，使检查更加严格 ● **ppp-max-payload** *value*：可选参数，指定 PPPoE 会话建立过程中，PPP 协商的 MTU 的最大值，取值范围为 64～1 976 的整数字节。缺省情况下，PPPoE 会话建立过程，PPP 协商的 MTU 最大值为 1 492 字节 缺省情况下，未指定 PPPoE 会话对应的 Dialer Bundle，可用 **undo pppoe-client dial-bundle-number** 命令删除 PPPoE 会话和 Dialer Bundle 的对应关系。但无论 PPPoE 会话工作在永久在线方式或报文触发方式，使用 **undo pppoe-client dial-bundle-number** 命令都会永久删除 PPPoE 会话。如果需要重新建立 PPPoE 会话，用户需要重新配置 【说明】在一个以太网接口或 Pon 接口上可以配置多个 PPPoE 会话，即一个以太网接口或 Pon 接口可以同时属于多个 Dialer Bundle，但是一个 Dialer Bundle 中只能拥有一个以太网接口或 Pon 接口。PPPoE 会话是和 Dialer Bundle 一一对应的。如果某一 Dialer 接口的 Dialer Bundle 已经有一个以太网接口或 Pon 接口被用于 PPPoE，那么此 Dialer Bundle 中不能加入其他任何接口。同样，如果在 Dialer Bundle 中已经有除 PPPoE 以太网接口或 Pon 接口以外的接口，那么此 Dialer Bundle 也同样不能加入被用于 PPPoE 客户端的以太网接口或 Pon 接口

表 4-22 通过 ATM 接口连接直接连入 Internet 时的 PPPoE 配置

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface virtual-ethernet** *ve-number* 例如：[Huawei] **interface virtual-ethernet** 0/0/12	创建并进入 VE（虚拟以太网）接口视图。参数 *ve-number* 用来指定虚拟以太网接口的编号。编号格式为槽号/卡号/顺序号，其中的“槽号/卡号”是与对应的物理接口卡一致的（也就是 ADSL 接口卡的位置）。AR150/150-S/200/200-S 系列、AR1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 的顺序号取值范围是 0～127 的整数；AR2220L、AR2220/2220-S、AR2240/2240-S 和 AR3200 的顺序号取值范围是 0～1 023 的整数

（续表）

步骤	命令	说明
3	**pppoe-client dial-bundle-number** *number* [**on-demand**] [**no-hostuniq**]　[**ppp-max-payload** *value*] 例如：[Huawei-GigabitEthernet1/0/0]**pppoe-client dial-bundle-number** 1	建立一个 PPPoE 会话，并指定 PPPoE 会话对应的 Dialer Bundle。其他说明参见表 4-21 中的第 3 步
4	**quit** 例如：[Huawei-GigabitEthernet1/0/0] **quit**	退出接口视图，返回系统视图
5	**interface atm** *interface-number* [*.subinterface*] 例如：[Huawei] **interface atm** 1/0/0	进入 ATM（子）接口视图。如果所选用的 ADSL 接口只用于创建一个 PPPoE 会话，则直接用主接口；如果在一个 ADSL 接口上要配置多个 PPPoE 会话，才需要创建子接口
6	**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* } 例如：[Huawei-Atm1/0/0] **pvc** huawei 1/101	创建一条或批量创建指定 VPI/VCI 的 PVC，并进入 PVC 视图。命令中的参数说明如下 ● *pvc-name*：指定 PVC 名，每条 PVC 的 *vpi/vci* 值对在一个 ATM 接口（包括主接口和子接口）范围内唯一 ● *vpi/vci*：指定对应 PVC 的 VPI（虚路径标识，取值范围为 0～255 的整数）和 VCI（虚通道标识，取值范围为 0～2 和 5～255）值，由 ISP 提供 缺省情况下，不创建任何 PVC，可用 **undo pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }命令删除指定的 PVC
7	**map bridge virtual-ethernet** *interface-number* 例如：[Huawei-Atm1/0/0] **map bridge virtual-ethernet** 0/0/12	创建 PVC 上的 PPPoEoA 映射，即将对应的 ATM 接口与前面创建的 VE 接口绑定

4.8.4　配置设备作为 PPPoE 服务器

路由器的 PPPoE 服务器功能可以配置在物理以太网接口或 PON 接口上，也可以配置在由 ADSL 接口生成的虚拟以太网接口上。主要包括的配置任务如下。

1. 配置虚拟模板接口

虚拟模板接口 VT 和以太网接口或 PON 接口绑定后，实现 PPPoE 功能。具体配置步骤如表 4-23 所示。

表 4-23　　PPPoE 服务器的虚拟模板接口配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface virtual-template** *vt-number* 例如：[Huawei] **interface virtual-template** 10	创建虚拟模板接口并进入虚拟模板接口视图。参数 *vt-number* 用来指定虚拟模板接口的编号，取值范围为 0～1 023 的整数 PPP、ATM 等二层协议之间不能直接互相承载，需要通过虚拟访问接口 VA（Virtual-Access）进行通信

（续表）

<table>
<tr><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td>3</td><td>**ppp authentication-mode** { **chap** | **pap** } [[**call-in**] domain *domain-name*]
例如：[Huawei-Virtual-Template10] **ppp authentication-mode chap**</td><td colspan="2">配置本端设备对对端设备的认证方式。命令中的参数和选项说明如下
● **chap**：二选一选项，指定本端设备对对端设备采用CHAP认证方式
● **pap**：二选一选项，指定本端设备对对端设备采用PAP认证方式
● **call-in**：可选项，指定只在远端用户呼入时才认证对方
● **domain** *domain-name*：可选参数，指定用户认证采用的域名，1～64个字符，不支持空格，**区分大小写**，不能使用星号“*”、问号“?”、引号“"”等
缺省情况下，本端设备对对端设备不进行认证，可用 **undo ppp authentication-mode** 命令恢复为缺省情况</td></tr>
<tr><td>4</td><td>**ip address** *ip-address* { *mask* | *mask-length* }
例如：[Huawei-Virtual-Template10] **ip address** 192.168.1.1 24</td><td colspan="2">配置虚拟模板接口的IPv4地址。本命令已在本章多次介绍，不再赘述</td></tr>
<tr><td rowspan="4">5</td><td>**remote address** *ip-address*
例如：[Huawei-Virtual-Template10] **remote address** 192.168.1.2 24</td><td>（二选一）配置直接为对端指定IP地址</td><td>配置为以上接口所连接的PPPoE客户端分配的IP地址
本种IP地址分配方式仅适用于单个客户端连接时
缺省情况下，本端不为对端分配IP地址，可用 **undo remote address** 命令恢复为缺省值</td></tr>
<tr><td>**remote address pool** *pool-name*
例如：[Huawei-Virtual-Template10]**remote address pool** global1</td><td rowspan="3">（二选一）配置通过使用全局地址池给对端分配地址</td><td>配置为PPPoE客户端分配指定地址池，参数 *pool-name* 用来指定为对端分配IP地址的地址池，即将指定地址池中的一个IP地址分配给对端，1～64个字符，不支持空格，**区分大小写**
本种IP地址分配方式适用于单个或者多个客户端连接时
缺省情况下，本端不为对端分配IP地址，可用 **undo remote address** 命令恢复为缺省值</td></tr>
<tr><td>**ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]
例如：[Huawei-Virtual-Template10] **ppp ipcp dns** 1.1.1.1</td><td>配置设备为对端设备指定主、从DNS服务器的IP地址。命令中的参数说明如下。
● *primary-dns-address*：为对端设备配置主DNS服务器IP地址
● *secondary-dns-address*：可选参数，为对端设备配置从DNS服务器IP地址
【说明】当主机与设备通过PPP相连时，主机若想通过域名直接访问Internet，则需要设备为主机指定DNS服务器地址
缺省情况下，设备不为对端设备指定DNS服务器的IP地址，可用 **undo ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]命令删除设备为对端设备配置的指定主、从DNS服务器IP地址</td></tr>
<tr><td>**quit**</td><td>退出VT接口视图，返回系统视图</td></tr>
</table>

（续表）

<table>
<tr><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td rowspan="3"></td><td>ip pool ip-pool-name
例如：[Huawei] ip pool global1</td><td rowspan="3">（二选一）配置通过使用全局地址池给对端分配地址</td><td>创建全局地址池并进入全局地址池视图。参数 ip-pool-name 指定前面用于为客户端分配 IP 地址的地址池名称</td></tr>
<tr><td>network ip-address [mask { mask | mask-length }]
例如：[Huawei-ip-pool-global1] network 192.168.1.0</td><td>配置地址池下的 IP 地址范围。命令中的参数说明如下
● ip-address：指定地址池中的网段地址（是一个网络地址）
● mask | mask-length：可选参数，指定以上网段地址对应的子网掩码（选择 mask 参数时）或子网掩码长度（选择 mask-length 参数时）。如果不指定此可选参数，则使用以上网段 IP 地址所对应的自然网段子网掩码
缺省情况下，系统未配置全局地址池下动态分配的 IP 地址范围，可用 undo network 命令恢复网段地址为缺省值</td></tr>
<tr><td>gateway-list ip-address &<1-8>
例如：[Huawei-ip-pool-global1] gateway-list 192.168.1.1</td><td>配置地址池的出口网关地址。参数 ip-address &<1-8>用来指定客户端的网关 IP 地址，最多可 8 个，用空格分隔
缺省情况下，没有配置出口网关地址，可用 undo gateway-list { ip-address | all } 命令删除指定的，或者全部（选择二选一选项 all 时）的网关 IP 地址配置</td></tr>
</table>

2. 配置接口上启用 PPPoE 服务器协议

用户需要将虚拟接口模板绑定到接口（物理以太网接口或 PON 接口，或者由 ADSL 接口生成的虚拟以太网接口），才可以实现 PPPoE 功能。具体配置步骤很简单，就是通过 **pppoe-服务器 bind virtual-template** *vt-number* 接口视图命令绑定连接客户端的路由器接口，但这里 *vt-number* 的参数值一定要与前面创建的 VT 接口编号一致。

3. （可选）配置 PPPoE 会话参数

为了保证 PPPoE 服务器的处理能力，管理员可以对 PPPoE 会话数的最大值进行配置，包括 PPPoE 服务器能创建 PPPoE 会话的最大数目、PPPoE 服务器的一个 MAC 地址上能创建的 PPPoE 会话的最大数目和 PPPoE 客户端的一个 MAC 地址上能创建 PPPoE 会话的最大数目。但这些都有对应的缺省值，故为可选配置任务。具体配置步骤如表 4-24 所示。

表 4-24　　PPPoE 会话参数配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**pppoe-server max-sessions total** *number* 例如：[Huawei] **pppoe-server max-sessions total** 120	配置设备能创建 PPPoE 会话的最大数目，取值范围如下：AR150/160/200 系列为 1～16 的整数；AR150-S 系列为 1～32 的整数；AR200-S/1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 为 1～128 的整数；AR2220L、AR2220/2220-S 和 AR2240 为 1～512 ；AR3200 系列为 1～1 024 的整数；对于 AR2240-S，不同

（续表）

步骤	命令	说明
2	**pppoe-server max-sessions total** *number* 例如：[Huawei] **pppoe-server max-sessions total** 120	的主控板取值范围不同：SRU40 和 SRU60 为 1～512 的整数，SRU80 为 1～1 024 的整数 缺省情况下，AR150/200 系列为 16；AR150-S 系列为 32，AR200/1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 为 128；AR2220L、AR2220/2200-S 和 AR2240 为 512；AR3200 系列为 1 024，对于 AR2240-S，不同的主控板取值范围不同：SRU40 和 SRU60 为 512，SRU80 为 1 024，可用 **undo pppoe-server max-sessions total** 命令恢复为缺省值
3	**pppoe-server max-sessions local-mac** *number* 例如：[Huawei] **pppoe-server max-sessions local-mac** 20	配置在一个本端 MAC 地址上能创建的 PPPoE 会话的最大数，取值范围如下：AR150/150-S/200 系列为 1～16 的整数；AR200/1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 为 1～128 的整数；AR2220L、AR2220/2220-S 和 AR2240 为 1～512 的整数；AR3200 系列为 1～ 的整数，对于 AR2240-S，不同的主控板取值范围不同：SRU40 和 SRU60 为 1～512 的整数，SRU80 为 1～1 024 的整数 缺省情况下，AR150/150-S/200 系列为 16；AR200-S/1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 为 128；AR2220L、AR2220/2220-S 和 AR2240 为 512；AR3200 系列为 1 024，对于 AR2240-S，不同的主控板取值不同：SRU40 和 SRU60 为 512，SRU80 为 1 024，可用 **undo pppoe-server max-sessions local-mac** 命令恢复为缺省值
4	**pppoe-server max-sessions remote-mac** *number* 例如：[Huawei] **pppoe-server max-sessions remote-mac** 15	配置在一个对端 MAC 地址上能创建 PPPoE 会话的最大数，取值范围如下：AR150/150-S/200/200-S 系列为 1～16 的整数；AR1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 为 1～128 的整数；AR2220L、AR2220/2220-S 和 AR2240/2240-S 为 1～512 的整数；AR3200：1～1 024 的整数 缺省情况下，AR150/150-S/200/200-S 为 16；AR1200/1200-S、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 为 128；AR2220L、AR2220/2220-S 和 AR2240/2240-S 为 512；AR3200 为 1 024，可用 **undo pppoe-server max-sessions remote-mac** 命令恢复为缺省值

4. 配置 PPPoE 认证用户

当设备作为 PPPoE 服务器对 PPPoE 客户端进行认证、授权和计费时，需配置 PPPoE 认证用户。这里仅以本地认证方式为例进行介绍。有关 AAA 认证、授权和计费参见配套图书《**华为交换机学习指南**》中的第 17 章。

本地 PPPoE 认证用户的配置是在 AAA 视图下进行的，具体如表 4-25 所示。

表 4-25 本地 PPPoE 认证用户的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**aaa** 例如：[Huawei] **aaa**	进入 AAA 视图

（续表）

步骤	命令	说明
3	**local-user** *user-name* **password cipher** *password* 例如：[Huawei-aaa]**local-user user1**@vipdomain **password cipher** huawei	创建一个本地 PPPoE 认证用户。命令中的参数说明如下 • *user-name*：指定创建的 PPPoE 认证用户名，1～64 个字符，不支持空格，区分大小写，格式“user@domain”。查询与修改时可以使用通配符“*”，例如*@isp、user@*、*@*。如果用户名中带域名分隔符，如@，则认为@前面的部分是用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域为默认域 • **cipher** *password*：指定 PPPoE 认证用户密码。如果是创建新用户，建议在创建用户的同时设置口令。**cipher** 表示以密文形式显示用户口令，并且在查看配置文件时将以密文方式显示密码 缺省情况下，系统中存在一个名称为“admin”的本地用户，该用户的密码为“vlan”，可用 **undo local-user** *user-name* 命令删除指定的本地用户
4	**local-user** *user-name* **service-type ppp** 例如：[Huawei-aaa]**local-user** user1@vipdomain **service-type ppp**	配置以上本地 PPPoE 认证用户的接入类型为 PPP 缺省情况下，本地用户可以使用所有的接入类型，可用 **undo local-user** *user-name* service-type 命令将指定的本地用户的接入类型恢复为缺省配置

4.8.5 PPPoE 管理

配置好 PPPoE 后，可用以下 **display** 任意视图命令查看相关配置，验证配置结果。

① **display access-user**：查看当前在线用户信息。

② **display pppoe-client session** { **packet** | **summary** } [**dial-bundle-number** *number*]：查看 PPPoE 客户端的 PPPoE 会话状态和统计信息。

③ **display pppoe-server session** { **all** | **packet** }：查看 PPPoE 会话状态和统计信息。

还可在 PPPoE 服务器用户视图下，执行 **reset pppoe-server** { **all** | **interface** *interface-type interface-number* | **virtual-template** *number* }命令清除 PPPoE 会话。

在 PPPoE Client 端用户视图下，执行 **reset pppoe-client** { **all** | **dial-bundle-number** *number* }命令复位 PPPoE 会话。

说明　当 PPPoE 会话工作在永久在线方式时，如果使用 **reset pppoe-client** 命令终止 PPPoE 会话，设备会在 16 s 后自动重新建立 PPPoE 会话。

当 PPPoE 会话工作在报文触发方式时，如果使用 **reset pppoe-client** 命令终止 PPPoE 会话，设备会在有数据需要传送时，才重新建立 PPPoE 会话。

也可在 AAA 视图下执行 **cut access-user user-id** *begin-number* [*end-number*] 命令强制断开指定 ID 的 PPPoE 会话。

4.8.6 设备作为 PPPoE 服务器的配置示例

本示例的基本网络结构参见图 4-19，局域网内主机与设备直连，设备作为 PPPoE 服务器，企业网内的主机需要通过 PPPoE 拨号接入 Internet。用户在主机上安装拨号软件，每个主机使用同一个账号进行拨号上网。用户需求如下。

- PPPoE 服务器为主机动态分配 IP 地址。
- PPPoE 服务器通过 AAA 本地认证认证主机用户。
- PPPoE 服务器为主机分配 DNS 服务器地址。

1. 基本配置思路分析

根据本示例的要求以及 4.8.4 小节中的配置方法（PPPoE 参数可不用配置，直接采用各自的缺省值），可以得出以下基本配置思路。

① 配置通过使用全局地址池给对端分配地址，实现 PPPoE 服务器为主机动态分配 IP 地址的目的。

② 配置 PPPoE 认证用户，实现 PPPoE 服务器对用户主机的认证要求。

③ 配置 PPPoE 服务器为对端设备指定 DNS 服务器的 IP 地址。

2. 具体配置步骤

① 创建并配置 VT。

```
<Router> system-view
[Router] interface virtual-template 1
[Router-Virtual-Template1] ppp authentication-mode chap domain system
[Router-Virtual-Template1] ip address 192.168.10.1 255.255.255.0
[Router-Virtual-Template1] remote address pool pool1
[Router-Virtual-Template1] ppp ipcp dns 10.10.10.10 10.10.10.11
[Router-Virtual-Template1] quit
```

② 配置用于为客户端分配 IP 地址的全局地址池 pool1。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] ip pool pool1
[Router-ip-pool-pool1] network 192.168.10.10 mask 255.255.255.0
[Router-ip-pool-pool1] gateway-list 192.168.10.1
[Router-ip-pool-pool1] quit
```

③ 在以太网接口 GE1/0/0 上启用 PPPoE 协议。

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] pppoe-server bind virtual-template 1
[Router-GigabitEthernet1/0/0] quit
```

④ 配置 PPPoE 认证用户。

```
[Router] aaa
[Router-aaa] authentication-scheme system_a
[Router-aaa-authen-system_a] authentication-mode local
[Router-aaa-authen-system_a] quit
[Router-aaa] domain system
[Router-aaa-domain-system] authentication-scheme system_a
[Router-aaa-domain-system] quit
[Router-aaa] local-user user1@system password cipher huawei2012
[Router-aaa] local-user user1@system service-type ppp
[Router-aaa] quit
```

配置完成后，可以在 PPPoE 服务器上执行 **display pppoe-server session all** 命令，显示 PPPoE 会话的状态信息和配置信息。根据显示信息判断会话状态是否正常（状态为 UP 表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

```
[Router] display pppoe-server session all
SID Intf                      State OIntf        RemMAC          LocMAC
10  Virtual-Template1:0        UP    GE1/0/0      0011.0914.1bd3 00e0.fc99.9999
```

4.8.7　设备作为 PPPoE 客户端的配置示例

本示例的基本网络结构如图 4-20 所示，路由器下行通过 GE1/0/0 连接局域网用户，上行通过 GE2/0/0 接入 PPPoE 服务器。用户希望这些主机共用一个账号，在建立连接过程中，通过这个账号到 PPPoE 服务器进行认证，认证通过后，即建立了一个 PPPoE 会话，接入 Internet；要求当长时间无数据传输时，PPPoE 客户端可以切断本次会话，当再有数据需要传输时，再建立会话。

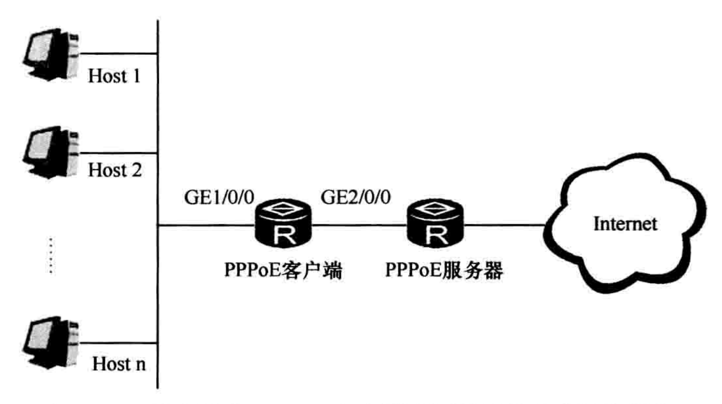


图 4-20　设备作为 PPPoE 客户端配置示例的基本网络结构

1. 基本配置思路分析

本示例其实同时涉及 PPPoE 客户端和 PPPoE 服务器的配置。在 PPPoE 客户端，根据 4.8.3 小节介绍的配置方法，针对本示例采用内置 ADSL Modem 方式，主要的配置任务如下。

① 配置 ADSL 接口属性，这方面可参见本书 3.12 小节。

② 配置 Dialer 接口：包括 Dialer 接口 IP 地址、PPP 封装、Dialer 接口属性和共享 DCC 拨号参数（包括 CHAP 认证，以实现设备通过 PPP 认证与 PPPoE 服务器建立连接），同时配置拨号方式为报文触发方式，实现用户希望当长时间无数据传输时，PPPoE 客户端可以切断本次会话，当再有数据需要传输时，再建立会话的要求。

③ 配置物理拨号接口：因为是采用以太网接口与 PPPoE 服务器连接，所以可以启用 PPPoE 协议，建立 PPPoE 会话连接。

PPPoE 服务器需要配置认证方式、IP 地址获取方式或设置为 PPPoE 客户端分配的 IP 地址或地址池。具体参见上节介绍。

下面仅介绍 PPPoE 客户端的配置。

2. 具体配置步骤

① 配置 Dialer 接口，主要是共享 DCC 配置，具体命令参见本章 4.3.2 小节和 4.3.3 小节。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dialer-rule
[Router-dialer-rule] dialer-rule 1 ip permit
[Router-dialer-rule] quit
```

```
[Router] interface dialer 1
[Router-Dialer1] dialer user user2
[Router-Dialer1] dialer-group 1
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] ppp chap user user1@system
[Router-Dialer1] ppp chap password cipher huawei
[Router-Dialer1] dialer timer idle 300
INFO:   The configuration will become effective after link reset.
[Router-Dialer1] dialer queue-length 8
[Router-Dialer1] ip address ppp-negotiate
[Router-Dialer1] quit
```

② 配置物理拨号接口，建立按需拨号 PPPoE 会话。

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] pppoe-client dial-bundle-number 1 on-demand
[Router-GigabitEthernet2/0/0] quit
```

③ 配置到 PPPoE 服务器的静态路由。

```
[Router] ip route-static 0.0.0.0 0 dialer1
```

配置好后，执行命令 **display pppoe-client session summary** 查看 PPPoE 会话的状态和配置信息。根据显示信息判断会话状态是否正常（状态为 UP 表示正常）、配置是否正确。

```
[Router] display pppoe-client session summary
PPPoE Client Session:
ID    Bundle   Dialer   Intf           Client-MAC      Server-MAC      State
1     1        1        GE2/0/0        00e0fc030201    0819a6cd0680    UP
```

4.8.8 利用 ADSL Modem 将局域网接入 Internet 的配置示例

本示例的拓扑结构如图 4-21 所示。RouterA 下行通过 Eth3/0/0 连接局域网用户，上行通过 GE1/0/0 连接 ADSL Modem 设备；RouterB 通过 ATM1/0/0 接口连接 DSLAM 设备。

已知局域网内计算机的内网地址的网段为 192.168.10.0/24，用户希望局域网内的计算机通过 RouterA 访问服务器 RouterB，并且希望局域网内的用户可以访问外网。已知账户的用户名为 user1，密码为 123456。

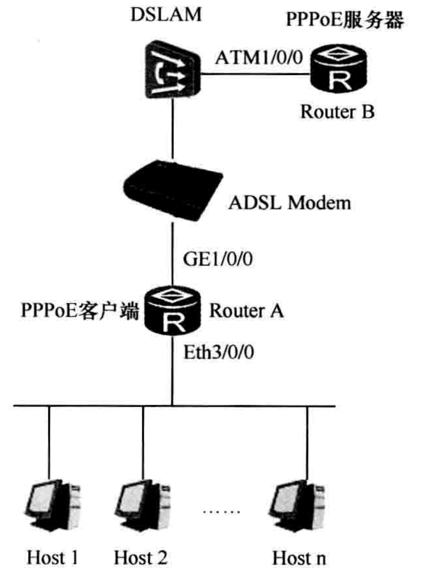


图 4-21 利用 ADSL Modem 将局域网接入 Internet 配置示例的基本网络结构

1. 基本配置思路分析

根据本示例的要求可以得出本示例的基本配置思路如下。

① 配置 RouterA 作为 PPPoE 客户端，实现局域网内的主机不用安装 PPPoE 客户端软件即可访问 Internet 的目的。这方面可直接参见上节介绍的示例，但本示例采用外置 ADSL Modem 连接方式，无需配置 ADSL 接口。

② 配置 RouterB 作为 PPPoE 服务器提供 RADIUS 认证、计费功能。

③ 配置 NAT 功能，实现局域网内的用户可以访问外网的目的。

2. 具体配置步骤

（1）PPPoE 客户端上的配置

① 配置 Dialer 拨号口。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
[RouterA] interface dialer 1
[RouterA-Dialer1] dialer user user1
[RouterA-Dialer1] dialer-group 1
[RouterA-Dialer1] dialer bundle 1
[RouterA-Dialer1] ppp chap user user1
[RouterA-Dialer1] ppp chap password simple 123456
[RouterA-Dialer1] dialer timer idle 300
[RouterA-Dialer1] dialer queue-length 8
[RouterA-Dialer1] ip address ppp-negotiate
[RouterA-Dialer1] quit
```

② 建立 PPPoE 会话。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pppoe-client dial-bundle-number 1
[RouterA-GigabitEthernet2/0/0] quit
```

③ 配置局域网用户通过 NAT 转换将私网地址转换为公网地址，进行拨号上网。

```
[RouterA] acl number 2002
[RouterA-acl-adv-2002] rule 5 permit ip source 192.168.10.0 0.0.0.255
[RouterA-acl-adv-2002] quit
[RouterA] interface dialer 1
[RouterA-Dialer1] nat outbound 2002
[RouterA-Dialer1] quit
```

④ 配置到 PPPoE 服务器的静态路由。假设 PPPoE 服务器的 IP 地址为 192.168.10.1。

```
[RouterA] ip route-static 0.0.0.0 0 dialer1
```

（2）PPPoE 服务器上的配置

① 配置全局地址池 pool1。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] ip pool pool1
[RouterB-ip-pool-pool1] network 192.168.10.10 mask 255.255.255.0
[RouterB-ip-pool-pool1] gateway-list 192.168.10.1
[RouterB-ip-pool-pool1] quit
```

② 创建并配置 VT。

```
<RouterB> system-view
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ppp authentication-mode chap domain system
[RouterB-Virtual-Template1] ip address 192.168.10.1 255.255.255.0
[RouterB-Virtual-Template1] remote address pool pool1
[RouterB-Virtual-Template1] quit
```

③ 在 Virtual Ethernet 接口上启用 PPPoE 服务器协议。

```
[RouterB] interface virtual-ethernet 0/0/1
[RouterB-Virtual-Ethernet0/0/1] pppoe-server bind virtual-template 1
[RouterB-Virtual-Ethernet0/0/1] quit
```

④ 对 ATM 接口进行配置。

```
[RouterB] interface atm 1/0/0
[RouterB-Atm1/0/0] pvc 0/32
[RouterB-Atm1/0/0-0/32] map bridge vrtual-ethernet 1
[RouterB-Atm1/0/0-0/32] quit
```

⑤ 配置 PPPoE 用户。

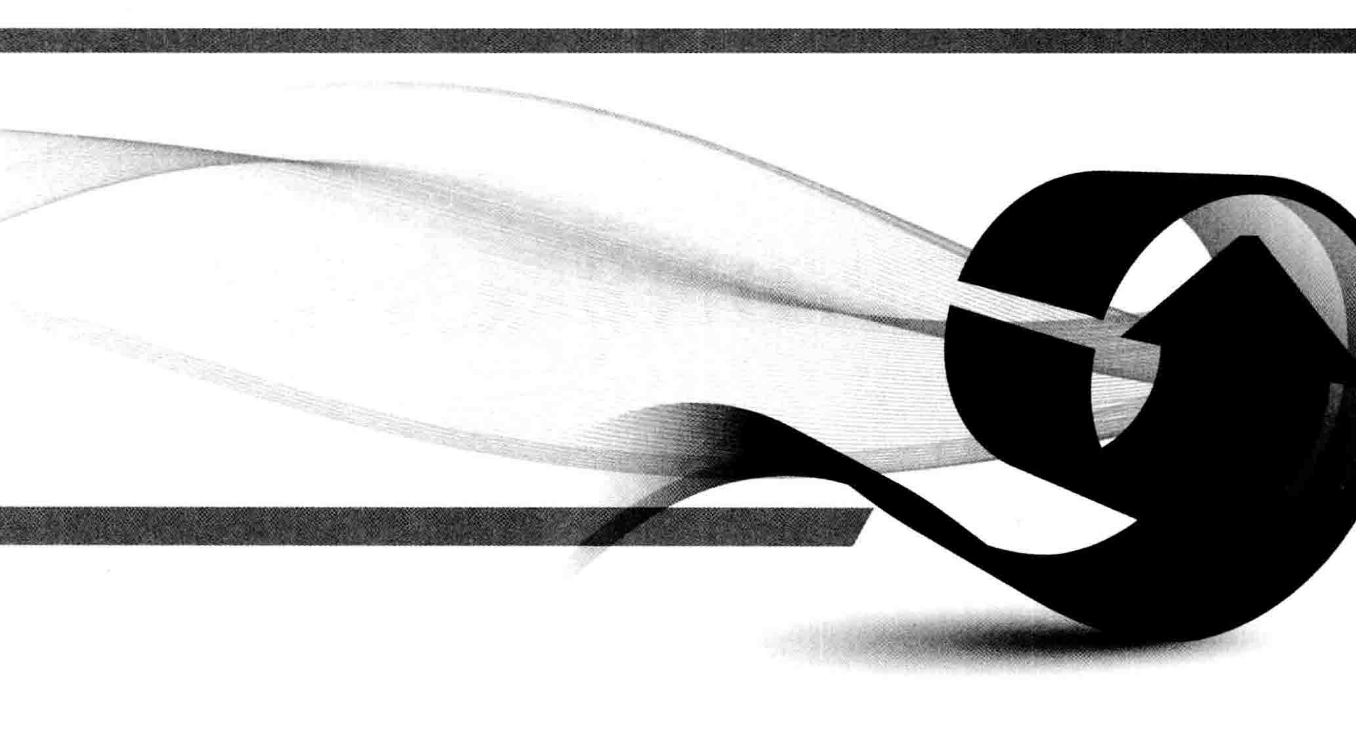
```
[RouterB] aaa
[RouterB-aaa] local-user user1 password cipher huawei2012
[RouterB-aaa] local-user user1 service-type ppp
[RouterB-aaa] quit
```

⑥ 配置 RADIUS 认证，计费方案。有关 RADIUS 的 AAA 认证、计费方案的配置方法参见配套图书《华为交换机学习指南》第 17 章。

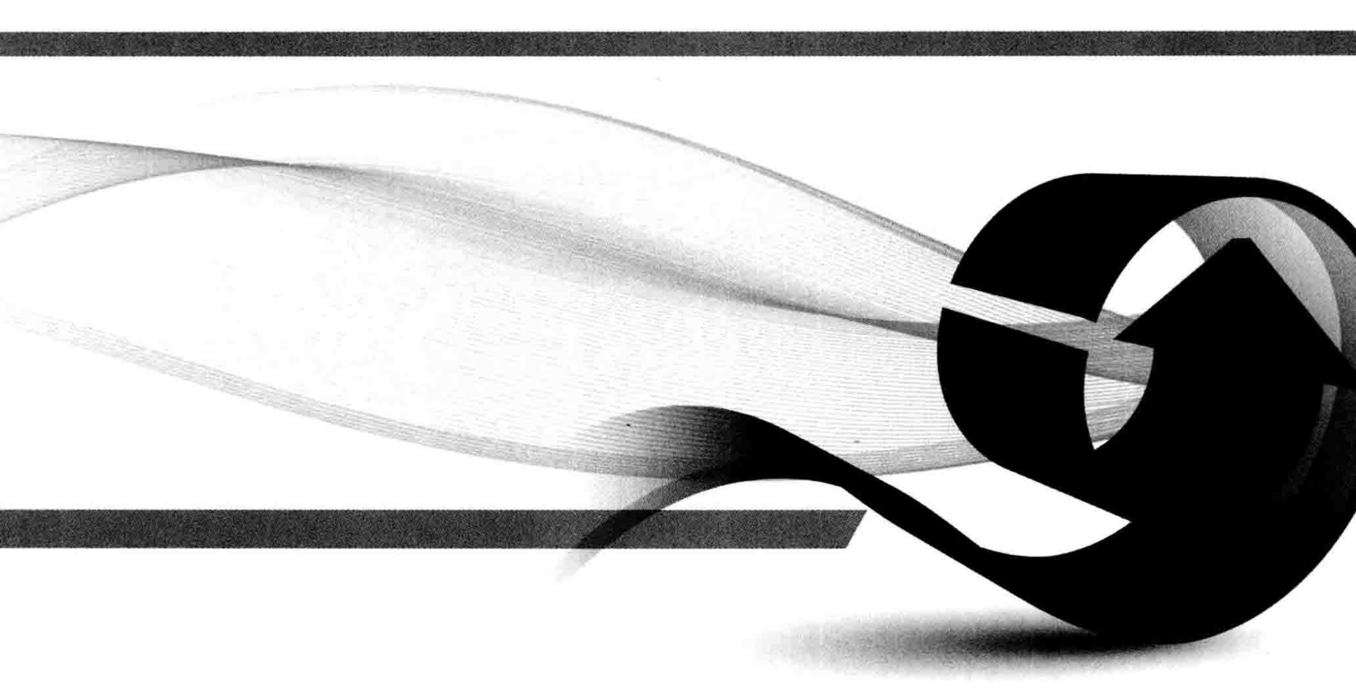
```
[RouterB] radius-server template shiva   !---创建 RADIUS 服务器模板
[RouterB-radius-shiva] radius-server authentication 129.6.6.66 1812 !---配置主 RADIUS 认证服务器地址和端口
[RouterB-radius-shiva] radius-server accounting 129.6.6.66 1813  !---配置主 RADIUS 计费服务器地址和端口
[RouterB-radius-shiva] radius-server authentication 129.6.6.67 1812 secondary  !---配置从 RADIUS 认证服务器地址和端口
[RouterB-radius-shiva] radius-server accounting 129.6.6.67 1813 secondary !---配置从 RADIUS 计费服务器地址和端口
[RouterB-radius-shiva] radius-server shared-key simple hello  !---配置 RADIUS 服务器共享密钥
[RouterB-radius-shiva] quit
[RouterB] aaa
[RouterB-aaa] authentication-scheme 1                    !---创建 AAA 认证方案
[RouterB-aaa-authen-1] authentication-mode radius        !---指定以上 AAA 认证方案采用 RADIUS 认证
[RouterB-aaa-authen-1] quit
[RouterB-aaa] accounting-scheme 1                        !---创建 AAA 计费方案
[RouterB-aaa-accounting-1] accounting-mode radius        !---指定以上 AAA 计费方案采用 RADIUS 计费
[RouterB-aaa-accounting-1] quit
[RouterB-aaa] domain system                              !---创建名为 system 的域
[RouterB-aaa-domain-system] authentication-scheme 1      !---指定在以上域中采用 1 认证方案
[RouterB-aaa-domain-system] accounting-scheme 1          !---指定在以上域中采用 1 计费方案
[RouterB-aaa-domain-system] radius-server shiva          !---指定以上域使用的 RADIUS 服务器模板
```

配置好后可以在 RouterA 上执行 **display pppoe-client session summary** 命令查看 PPPoE 会话的状态和配置信息。根据显示信息判断会话状态是否正常（状态为 UP 表示正常）、配置是否正确。

```
<RouterA> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC     Server-MAC    State
0    1       1       GE0/0/1       54899874dbc7   000000000000  PADI
```



第5章 DHCP/DNS服务配置与管理



本章主要介绍在AR G3系列路由器上配置DHCP和DNS这两个非常重要的服务，其中DHCP服务尤为重要。

DHCP服务看似比较简单，但功能非常强大，配置主要涉及DHCP服务器、DHCP中继、DHCP Snooping和DHCP客户端4大部分。在AR G3系列路由器上可以配置以上全部的4种角色，但主要是前三种，特别是DHCP服务器。在配置AR G3系列路由器担当DHCP服务器角色时，可以配置全局地址池和接口地址池这两种地址，以便适应不同的网络环境，满足不同的用户需求。DHCP Snooping功能非常实用，可以防止仿冒DHCP服务器的攻击（解决私设DHCP服务器的问题）、仿冒DHCP报文的攻击和DHCP服务器拒绝服务的攻击（解决合法用户无法获取IP地址的问题）等。

在DNS服务中，AR G3系列路由器可配置DNS客户端、DNS Proxy/Relay、DDNS客户端这三种角色，主要是后面两种。

5.1 DHCP 基础

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）技术实现了客户端 IP 地址和配置信息的动态分配以及集中管理，可以快速、动态地为用户分配和管理 IP 地址，保证 IP 地址的合理分配，提高 IP 地址使用效率。它采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息。

在以下场合通常利用 DHCP 服务来完成 IP 地址分配。

① 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。当然，各种服务器、网络设备节点都是需要采用静态 IP 地址分配的，否则用户可能无法访问你的服务器，网络设备也无法完成正常的数据转发和路由功能。

② 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。例如，Internet 接入服务提供商限制同时接入网络的用户数目，大量用户必须动态获得自己的 IP 地址。

③ 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

5.1.1 DHCP 概述

随着网络规模的扩大和网络复杂度的提高，网络配置变得越来越复杂，再加上用户计算机数量剧增且位置不固定（如移动便携机或无线网络），引发了 IP 地址变化频繁以及 IP 地址不足的问题。为了实现网络为用户主机动态、合理地分配 IP 地址，减轻管理员手动配置用户 IP 地址的工作负担，提高 IP 地址的利用率，可以使用 DHCP 服务来完成。它可以实现与手动配置用户 IP 地址方式一样的效果，包括为用户主机配置 IP 地址、子网掩码、缺省网关等网络参数。

DHCP 服务采用 Client/Server（客户端/服务器）模型结构，基本构架如图 5-1 所示，主要包括以下三种角色。

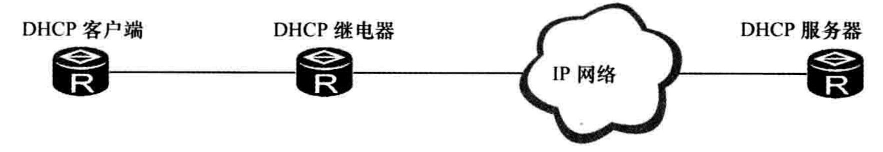


图 5-1 DHCP 服务的基本架构

1. DHCP Client（DHCP 客户端）

DHCP 客户端就是希望通过 DHCP 服务器（DHCP Server）获取 IP 地址信息分配的用户主机或者其他设备。

2. DHCP Server（DHCP 服务器）

DHCP 服务器负责处理来自客户端或中继的地址分配、地址续租、地址释放等请求，为客户端分配 IP 地址和其他网络配置信息。

3. DHCP Relay（DHCP 中继）

如果 DHCP 服务器和 DHCP 客户端不在同一个网段范围内（**如果 DHCP 服务器和**

DHCP 客户端在同一个网段，则不需要 DHCP 中继），则需要由 DHCP 中继负责 DHCP 服务器与 DHCP 客户端之间的 DHCP 报文转发。这样可以避免在每个网段范围内都部署 DHCP 服务器，既节省了成本，又便于进行集中管理。

华为 AR G3 系列路由器可作为 DHCP 服务器、DHCP 中继、DHCP 客户端使用。

5.1.2　DHCP 报文及其格式

DHCP 服务一样工作在 C/S（客户端/服务器）模式，但两者进行报文传输时所使用的 UDP 传输端口是不一样的，DHCP 客户端使用 68 号 UDP 端口发送请求报文；DHCP 服务器使用 67 号 UDP 端口发送应答报文。DHCP 客户端向 DHCP 服务器发送的报文称为 DHCP 请求报文，而 DHCP 服务器向 DHCP 客户端发送的报文称为 DHCP 应答报文。

1. DHCP 报文种类

整个 DHCP 服务一共有 8 种类型（主要是前面 7 种类型）的 DHCP 报文，分别为 DHCP Discover、DHCP Offer、DHCP Request、DHCP ACK、DHCP NAK、DHCP Release、DHCP Decline、DHCP Inform。以上这些类型报文基本功能如表 5-1 所示。

表 5-1　DHCP 报文类型

DHCP 报文类型	说明
DHCP DISCOVER	因为 DHCP 客户端在请求 IP 地址时并不知道 DHCP 服务器的位置，因此 DHCP 客户端会在本地网络内以广播方式发送 DISCOVER 请求报文，以发现网络中的 DHCP 服务器。所有收到 DISCOVER 报文的 DHCP 服务器都会发送应答报文，DHCP 客户端据此可以知道网络中存在的 DHCP 服务器的位置
DHCP OFFER	DHCP 服务器收到 DISCOVER 报文后，就会在所配置的地址池中查找一个合适的 IP 地址，加上相应的租约期限和其他配置信息（如网关、DNS 服务器等），构造一个 OFFER 报文，发送给 DHCP 客户端，告知用户本服务器可以为其提供 IP 地址。但这个报文只是告诉 DHCP 客户端可以提供 IP 地址，最终还需要客户端通过 ARP 来检测该 IP 地址是否重复
DHCP REQUEST	DHCP 客户端可能会收到很多 OFFER 请求报文，所以必须在这些应答中选择一个。通常是选择第一个 OFFER 应答报文的服务器作为自己的目标服务器，并向该服务器发送一个广播的 REQUEST 请求报文，通告选择的服务器，希望获得所分配的 IP 地址。另外，DHCP 客户端在成功获取 IP 地址后，在地址使用租期过去 1/2 时，也会向 DHCP 服务器发送单播 REQUEST 请求报文请求续延租约，如果没有收到 ACK 报文，在租期过去 3/4 时，会再次发送广播的 REQUEST 请求报文以请求续延租约
DHCP ACK	DHCP 服务器收到 Request 请求报文后，根据 REQUEST 报文中携带的用户 MAC 来查找有没有相应的租约记录，如果有则发送 ACK 应答报文，通知用户可以使用分配的 IP 地址
DHCP NAK	如果 DHCP 服务器收到 REQUEST 请求报文后，没有发现有相应的租约记录或者由于某些原因无法正常分配 IP 地址，则向 DHCP 客户端发送 NAK 应答报文，通知用户无法分配合适的 IP 地址
DHCP RELEASE	当 DHCP 客户端不再需要使用分配 IP 地址时，就会主动向 DHCP 服务器发送 RELEASE 请求报文，告知服务器用户不再需要分配 IP 地址，请求 DHCP 服务器释放对应的 IP 地址
DHCP DECLINE	DHCP 客户端收到 DHCP 服务器 ACK 应答报文后，通过地址冲突检测发现服务器分配的地址冲突或者由于其他原因导致不能使用，则会向 DHCP 服务器发送 DECLINE 请求报文，通知服务器所分配的 IP 地址不可用，以期获得新的 IP 地址

（续表）

DHCP 报文类型	说明
DHCP INFORM	DHCP 客户端如果需要从 DHCP 服务器端获取更为详细的配置信息，则向 DHCP 服务器发送 INFORM 请求报文；DHCP 服务器在收到该报文后，将根据租约查找到相应的配置信息后，向 DHCP 客户端发送 ACK 应答报文。目前基本上不用了

2. DHCP 报文格式

虽然 DHCP 服务的报文类型比较多，但每种报文的格式相同，不同类型的报文只是报文中的某些字段取值不同。DHCP 报文格式基于 BOOTP 的报文格式，具体格式如图 5-2 所示。下面是各字段的说明，至于各 DHCP 报文的具体取值参见下一节给出的示例。

0 7 15 23 31 bit

OP	Htype	Hlen	Hops
Xid			
Secs		Flags	
Ciaddr			
Yiaddr			
Siaddr			
Giaddr			
Giaddr (128位)			
Sname (512位)			
File (1024位)			
Options (可变长)			

图 5-2 DHCP 报文格式

① OP：Operation，指定 DHCP 报文的操作类型，占 8 位。请求报文置 1，应答报文置 2。表 5-1 中的 DHCP DISCOVER、DHCP REQUEST、DHCP RELEASE、DHCP INFORM 和 DHCP DECLINE 为请求报文，而 DHCP OFFER、DHCP ACK 和 DHCP NAK 为应答报文。

② Htype、Hlen：分别指定 DHCP 客户端的 MAC 地址类型和 MAC 地址长度，各占 8 位。MAC 地址类型其实用于指明网络类型，Htype 字段置 1 时表示为最常见的以太网 MAC 地址类型；以太网 MAC 地址长度为 6 字节，即对应 Hlen 字段值为 6。

③ Hops：指定 DHCP 报文经过的 DHCP 中继的数目，占 8 位。DHCP 请求报文每经过一个 DHCP 中继该字段就会增加 1。没有经过 DHCP 中继时值为 0。

④ Xid：客户端通过 DHCP Discover 报文发起一次 IP 地址请求时选择的随机数，相

当于请求标识（占 32 位），用来标识一次 IP 地址请求过程。在一次请求中所有报文的 Xid 都是一样的。

⑤ Secs：DHCP 客户端从获取到 IP 地址或者续约过程开始到现在所消耗的时间，以秒为单位，占 16 位。在没有获得 IP 地址前该字段始终为 0。

⑥ Flags：标志位，占 16 位，第一位为广播应答标识位，用来标识 DHCP 服务器应答报文是采用单播还是广播发送，置 0 时表示采用单播发送方式，置 1 时表示采用广播发送方式。其余位保留不用。

注意　在客户端正式分配了 IP 地址之前的第一次 IP 地址请求过程中，所有 DHCP 报文都是以广播方式发送的，包括客户端发送的 DHCP DISCOVER 和 DHCP REQUEST 报文以及 DHCP 服务器发送的 DHCP OFFER、DHCP ACK 和 DHCP NAK 报文。当然，如果是由 DHCP 中继器转的报文，则都是以单播方式发送的。另外，IP 地址续约、IP 地址释放的相关报文都是采用单播方式进行发送的。

⑦ Ciaddr：指示 DHCP 客户端的 IP 地址，占 32 位（4 个字节）。仅在 DHCP 服务器发送的 ACK 报文中显示，在其他报文中均显示 0.0.0.0，因为在得到 DHCP 服务器确认前，DHCP 客户端是还没有分配到 IP 地址的。

⑧ Yiaddr：指示 DHCP 服务器分配给客户端的 IP 地址，占 32 位（4 个字节）。仅在 DHCP 服务器发送的 OFFER 和 ACK 报文中显示，其他报文中显示为 0.0.0.0。

⑨ Siaddr：指示下一个为 DHCP 客户端分配 IP 地址等信息的 DHCP 服务器 IP 地址，占 32 位（4 个字节）。仅在 DHCP OFFER、DHCP ACK 报文中显示，其他报文中显示为 0.0.0.0。

⑩ Giaddr：指示 DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址，占 32 位（4 个字节）。如果没有经过 DHCP 中继，则显示为 0.0.0.0。

⑪ Chaddr：指示 DHCP 客户端的 MAC 地址，占 128 位（16 个字节）。在每个报文中都会显示对应 DHCP 客户端的 MAC 地址。

⑫ Sname：指示为 DHCP 客户端分配 IP 地址的 DHCP 服务器名称（DNS 域名格式），占 512 位（64 字节）。在 OFFER 和 ACK 报文中显示发送报文的 DHCP 服务器名称，其他报文显示为空。

⑬ File：指示 DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息，占 1 024 位（128 字节）。仅在 DHCP OFFER 报文中显示，其他报文中显示为空。

⑭ Option：可选字段，长度可变，最多为 312 字节。DHCP 通过此字段包含了 DHCP 报文类型，服务器分配给终端的配置信息，如网关 IP 地址、DNS 服务器的 IP 地址、客户端可以使用 IP 地址的有效租期等信息。

在此部分可选的选项包含：报文类型（代码为 53，占 1 字节）、有效租约期（代码为 51，以秒为单位，占 4 字节）、续约时间（代码为 58，占 4 字节）、子网掩码（代码为 1，占 4 字节）、默认网关（代码为 3，可以是一个路由器 IP 地址列表，长度可变，但必须是 4 字节的倍数）、DNS 服务器（代码为 6，可以是一个 DNS 服务器 IP 地址列表，长度可变，但必须是 4 字节的整数倍）、域名称（代码为 15，主 DNS 服务器名称，长度可变）、WINS 服务器（代码为 44，可以是一个 WINS 服务器 IP 列表，长度可变，但必须

是 4 字节的倍数）等配置信息。表 5-1 所示的 DHCP 报文类型的取值分别如下。

- DHCP DISCOVER：1
- DHCP OFFER：2
- DHCP REQUEST：3
- DHCP DECLINE：4
- DHCP ACK：5
- DHCP NAK：6
- DHCP RELEASE：7

5.1.3 DHCP 服务 IP 地址自动分配原理

DHCP 在提供服务时，DHCP 客户端是以 UDP 68 号端口进行数据传输的，而 DHCP 服务器是以 UDP 67 号端口进行数据传输的。DHCP 服务不仅体现在为 DHCP 客户端提供 IP 地址自动分配的过程中，还体现在后面的 IP 地址续约和释放的过程中。本节仅介绍 DHCP 客户端初次分配 IP 地址的过程。

在整个 DHCP 服务器为 DHCP 客户端初次提供 IP 地址自动分配过程中，一共经过了以下 4 个阶段，利用了表 5-1 中的前 4 个报文：发现阶段（DHCP 客户端在网络中广播发送 DHCP DISCOVER 请求报文，发现 DHCP 服务器，请求 IP 地址租约）、提供阶段（DHCP 服务器通过 DHCP OFFER 报文向 DHCP 客户端提供 IP 地址预分配）、选择阶段（DHCP 客户端通过 DHCP REQUEST 报文确认选择第一个 DHCP 服务器为它提供 IP 地址自动分配服务）和确认阶段（被选择的 DHCP 服务器通过 DHCP ACK 报文把在 DHCP OFFER 报文中准备的 IP 地址租约给对应 DHCP 客户端）。

DHCP 客户端在获得了一个 IP 地址以后，就可以发送一个免费 ARP 请求探测网络中是否还有其他主机使用 IP 地址，来避免由于 DHCP 服务器地址池重叠而引发的 IP 冲突。以上 4 个阶段如图 5-3 所示，相当于 DHCP 客户端与 DHCP 服务器的 4 次握手过程。具体描述如下。

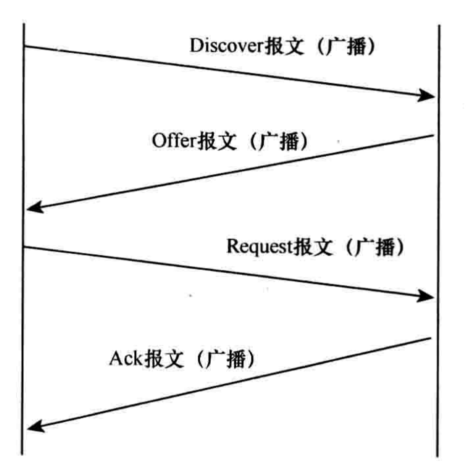


图 5-3 DHCP 客户端从 DHCP 服务器获取 IP 地址的四个阶段

1. 发现阶段

即 DHCP 客户端获取网络中 DHCP 服务器信息的阶段。在客户端配置了 DHCP 客户端程序并启动后，**以广播方式**发送 DHCP DISCOVER 报文来寻找网络中的 DHCP 服务器。此广播报文采用传输层的 UDP 68 号端口发送（封装的目的端口为 UDP 67 号端口），经过网络层 IP 协议封装后，源 IP 地址为 0.0.0.0（因为此时还没有分配 IP 地址），目的 IP 地址为 255.255.255.255（有限广播 IP 地址）。如下是一个 DHCP DISCOVER 报文封装的 IP 报头示例，可以看到 Destination Address（目的地址）是 255.255.255.255，而 Source Address（源地址）是 0.0.0.0。

```
IP:ID = 0x0; Proto = UDP; Len: 328
IP:Version = 4 (0x4)
IP:Header Length = 20 (0x14)
IP:Service Type = 0 (0x0)
IP:Precedence = Routine
IP:...0.... = Normal Delay
IP:....0... = Normal Throughput
IP:.....0.. = Normal Reliability
IP:Total Length = 328 (0x148)
IP:Identification = 0 (0x0)
IP:Flags Summary = 0 (0x0)
IP:.......0 = Last fragment in datagram
IP:......0. = May fragment datagram if necessary
IP:Fragment Offset = 0 (0x0) bytes
IP:Time to Live = 128 (0x80)
IP:Protocol = UDP - User Datagram              !---使用 UDP 传输层协议
IP:Checksum = 0x39A6
IP:Source Address = 0.0.0.0                    !---源 IP 地址为 0.0.0.0
IP:Destination Address = 255.255.255.255       !----目的 IP 地址为 255.255.255.255
IP:Data:Number of data bytes remaining = 308 (0x0134)
```

【经验之谈】在以上 DHCP DISCOVER 报文中 IP 报头的目的地址（Destination Address）是 255.255.255.255 这个有限广播地址。这个有限广播地址就是代表任意一个 IPv4 子网的广播地址，当然是发送报文的主机所在的子网和 DHCP 服务器所在子网的广播地址，因为此时 DHCP 客户端并不知道 DHCP 服务器所在的是哪个子网。下面所有其他 DHCP 报文中的 255.255.255.255 地址的含义也是一样的。

至于 IP 报头中的源地址（Source Address），由于当前 DHCP 客户端主机并未分配具体的 IP 地址，所以只能用具有任意代表功能的 0.0.0.0 地址来表示了。下面所有其他 DHCP 报文中指定的 0.0.0.0 地址的含义也是一样的。

因为此时，DHCP 客户端没有分配到 IP 地址，也不知道 DHCP 服务器或 DHCP 中继的 IP 地址，所以在 DHCP DISCOVER 报文中 Ciaddr（客户端 IP 地址）、Yiaddr（被分配的 DHCP 客户端 IP 地址）、Siaddr（下一个为 DHCP 客户端分配 IP 地址的 DHCP 服务器地址）、Giaddr（DHCP 中继 IP 地址）这 4 个字段均为 0.0.0.0，如下所示。另外，从中可以看到，在 Ciaddr 字段和 DHCP 选项中，Client Identifier 字段都标识了 DHCP 客户端网卡 MAC 地址。

```
DHCP:Discover              (xid=21274A1D)
DHCP:Op Code               (op)      = 1 (0x1)
DHCP:Hardware Type         (htype)   = 1 (0x1) 10Mb Ethernet
DHCP:Hardware Address Length (hlen) = 6 (0x6)
DHCP:Hops                  (hops)    = 0 (0x0)
DHCP:Transaction ID        (xid)     = 556223005 (0x21274A1D)
DHCP:Seconds               (secs)    = 0 (0x0)
DHCP:Flags                 (flags)   = 1 (0x1)    !---标志位置 1，代表以广播方式发送
DHCP:1............... = Broadcast
DHCP:Client IP Address (ciaddr) = 0.0.0.0
DHCP:Your    IP Address (yiaddr) = 0.0.0.0
DHCP:Server IP Address (siaddr) = 0.0.0.0
DHCP:Relay   IP Address (giaddr) = 0.0.0.0
DHCP:Client Ethernet Address (chaddr) = 08002B2ED85E
DHCP:Server Host Name    (sname)    = <Blank>
```

```
DHCP:Boot File Name      (file)      = <Blank>
DHCP:Magic Cookie = [OK]
DHCP:Option Field        (options)
DHCP:DHCP Message Type          = DHCP Discover     !---DHCP 报文类型为 DHCP Discover
DHCP:Client-identifier          = (Type:1) 08 00 2b 2e d8 5e
DHCP:Host Name                  = JUMBO-WS      !---DHCP 服务器主机名
DHCP:Parameter Request List = (Length:7) 01 0f 03 2c 2e 2f 06
DHCP:End of this option field
```

2. 提供阶段

即 DHCP 服务器向 DHCP 客户端提供预分配 IP 地址的阶段。网络中的所有 DHCP 服务器接收到客户端的 DHCP DISCOVER 报文后，都会根据自己地址池中 IP 地址分配的优先次序选出一个 IP 地址，然后与其他参数一起通过传输层的 UDP 67 号端口，在 DHCP OFFER 报文中**以广播方式**发送给客户端（目的端口是 DHCP 客户端的 UDP 68 号端口）。客户端通过封装在帧中的目的 MAC 地址（也就在 DHCP DISCOVER 报文中的 CHADDR 字段值）的比对来确定是否接收该帧。这样一来，理论上 DHCP 客户端可能会收到多个 DHCP OFFER 报文（当网络中存在多个 DHCP 服务器时），但 DHCP 客户端只接受第一个到来的 DHCP OFFER 报文。

DHCP OFFER 报文经过 IP 协议封装后的源 IP 地址为 DHCP 服务器自己的 IP 地址，目的地址仍是 255.255.255.255 广播地址，使用的协议仍为 UDP。下面是一个 DHCP OFFER 报文的 IP 报头示例。

```
IP:ID = 0x3C30; Proto = UDP; Len: 328
IP:Version = 4 (0x4)
IP:Header Length = 20 (0x14)
IP:Service Type = 0 (0x0)
IP:Precedence = Routine
IP:...0.... = Normal Delay
IP:....0... = Normal Throughput
IP:.....0.. = Normal Reliability
IP:Total Length = 328 (0x148)
IP:Identification = 15408 (0x3C30)
IP:Flags Summary = 0 (0x0)
IP:.......0 = Last fragment in datagram
IP:......0. = May fragment datagram if necessary
IP:Fragment Offset = 0 (0x0) bytes
IP:Time to Live = 128 (0x80)
IP:Protocol = UDP - User Datagram
IP:Checksum = 0x2FA8
IP:Source Address = 157.54.48.151
IP:Destination Address = 255.255.255.255
IP:Data:Number of data bytes remaining = 308 (0x0134)
```

在 DHCP OFFER 报文中，Ciaddr 字段值仍为 0.0.0.0，因为客户端仍没有分配到 IP 地址；Yiaddr 字段已有值了，这是 DHCP 服务器为该客户端预分配的 IP 地址；Siaddr 字段值为 DHCP 服务器地址；因为没有经过 DHCP 中继服务器，所以 Giaddr 字段值仍为 0.0.0.0。另外，在 DHCP 可选项部分，可以看到由服务器随 IP 地址一起发送的各种选项。在这种情况下，服务器发送的是子网掩码、默认网关（路由器）、租约时间、WINS 服务器地址（NetBIOS 名称服务）和 NetBIOS 节点类型。下面是一个 DHCP OFFER 报文示例。

```
DHCP:Offer                    (xid=21274A1D)
DHCP:Op Code                  (op)       = 2 (0x2)
DHCP:Hardware Type            (htype)    = 1 (0x1) 10Mb Ethernet
DHCP:Hardware Address Length (hlen) = 6 (0x6)
DHCP:Hops                     (hops)     = 0 (0x0)
DHCP:Transaction ID           (xid)      = 556223005 (0x21274A1D)
DHCP:Seconds                  (secs)     = 0 (0x0)
DHCP:Flags                    (flags)    = 1 (0x1)
DHCP:1............... =   Broadcast
DHCP:Client IP Address (ciaddr) = 0.0.0.0
DHCP:Your    IP Address (yiaddr) = 157.54.50.5
DHCP:Server IP Address (siaddr) = 157.54.48.151
DHCP:Relay   IP Address (giaddr) = 0.0.0.0
DHCP:Client Ethernet Address (chaddr) = 08002B2ED85E
DHCP:Server Host Name    (sname)    = JUMBO-WS
DHCP:Boot File Name      (file)     = <Blank>
DHCP:Magic Cookie = [OK]
DHCP:Option Field         (options)
DHCP:DHCP Message Type          = DHCP Offer              !---DHCP 报文类型为 DHCP Offer
DHCP:Subnet Mask                = 255.255.240.0           !---所分配 IP 地址的子网掩码为 255.255.240.0
DHCP:Renewal Time Value (T1) = 8 Days,   0:00:00          !---想要继续租约原来分配的 IP 地址，则提出续约申请的
期限为 8 天
DHCP:Rebinding Time Value (T2) = 14 Days,   0:00:00       !---如果上次申请续约失败，再次申请绑定原来分配到的 IP
地址的期限为 14 天
DHCP:IP Address Lease Time   = 16 Days,   0:00:00         !---租约期限为 16 天，也就是 DHCP 客户端可使用此 IP
地址的最长时间为 16 天
DHCP:Server Identifier         = 157.54.48.151            !---DHCP 服务器的 IP 地址为 157.54.48.151
DHCP:Router                    = 157.54.48.1              !---默认网关 IP 地址为 157.54.48.1
DHCP:NetBIOS Name Service      = 157.54.16.154            !---DNS 服务器 IP 地址为 157.54.16.154
DHCP:NetBIOS Node Type         = (Length: 1) 04
DHCP:End of this option field
```

3. 选择阶段

即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCP OFFER 报文，客户端只接受第一个收到的 DHCP OFFER 报文，然后以**广播方式**发送 DHCP REQUEST 报文。在该报文的“**Requested Address**”选项中包含 DHCP 服务器在 DHCP OFFER 报文中预分配的 IP 地址，对应的 DHCP 服务器 IP 地址等。这样也就相当于同时告诉其他 DHCP 服务器，它们可以释放已提供的地址，并将这些地址返回到可用地址池中。

在 DHCP REQUEST 报文封装的 IP 协议头部中，客户端的 Source Address 仍然是 0.0.0.0，数据包的 Destination 仍然是 255.255.255.255。但在 DHCP REQUEST 报文中 Ciaddr、Yiaddr、Siaddr、Giaddr 字段的地址均 0.0.0.0，大家自己分析一下为什么，很简单的。下面是一个 DHCP REQUEST 报文头部和 DHCP REQUEST 报文示例。

```
IP:ID = 0x100; Proto = UDP; Len: 328
IP:Version = 4 (0x4)
IP:Header Length = 20 (0x14)
IP:Service Type = 0 (0x0)
IP:Precedence = Routine
IP:...0.... = Normal Delay
IP:....0... = Normal Throughput
IP:.....0.. = Normal Reliability
IP:Total Length = 328 (0x148)
```

```
IP:Identification = 256 (0x100)
IP:Flags Summary = 0 (0x0)
IP:.......0 = Last fragment in datagram
IP:......0. = May fragment datagram if necessary
IP:Fragment Offset = 0 (0x0) bytes
IP:Time to Live = 128 (0x80)
IP:Protocol = UDP - User Datagram
IP:Checksum = 0x38A6
IP:Source Address = 0.0.0.0
IP:Destination Address = 255.255.255.255
IP:Data:Number of data bytes remaining = 308 (0x0134)

DHCP:Request                (xid=21274A1D)
DHCP:Op Code                (op)       = 1 (0x1)
DHCP:Hardware Type          (htype)    = 1 (0x1) 10Mb Ethernet
DHCP:Hardware Address Length (hlen) = 6 (0x6)
DHCP:Hops                   (hops)     = 0 (0x0)
DHCP:Transaction ID         (xid)      = 556223005 (0x21274A1D)
DHCP:Seconds                (secs)     = 0 (0x0)
DHCP:Flags                  (flags)    = 1 (0x1)
DHCP:1............... = Broadcast
DHCP:Client IP Address (ciaddr) = 0.0.0.0
DHCP:Your    IP Address (yiaddr) = 0.0.0.0
DHCP:Server IP Address (siaddr) = 0.0.0.0
DHCP:Relay   IP Address (giaddr) = 0.0.0.0
DHCP:Client Ethernet Address (chaddr) = 08002B2ED85E
DHCP:Server Host Name   (sname)   = <Blank>
DHCP:Boot File Name     (file)    = <Blank>
DHCP:Magic Cookie = [OK]
DHCP:Option Field          (options)
DHCP:DHCP Message Type          = DHCP Request
DHCP:Client-identifier         = (Type:1) 08 00 2b 2e d8 5e
DHCP:Requested Address          = 157.54.50.5
DHCP:Server Identifier         = 157.54.48.151
DHCP:Host Name                  = JUMBO-WS
DHCP:Parameter Request List = (Length:7) 01 0f 03 2c 2e 2f 06
DHCP:End of this option field
```

4. 确认阶段

即 DHCP 服务器确认分配级 DHCP 客户端 IP 地址的阶段。某个 DHCP 服务器在收到 DHCP 客户端发来的 DHCP REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认将地址分配给该客户端，则**以广播方式**返回 DHCP ACK 报文；否则返回 DHCP NAK 报文，表明地址不能分配给该客户端。

在 DHCP 服务器发送的 DHCP ACK 报文的 IP 协议头部中，Source Address 是 DHCP 服务器 IP 地址，Destination Address 仍然是广播地址 255.255.255.255。在 DHCP ACK 报文中的 Yiaddr 字段包含要分配给客户端的 IP 地址，而 Chaddr 和 DHCP:Client Identifier 字段是发出请求的客户端中网卡的 MAC 地址。同时，在选项部分也会把在 DHCP OFFER 报文中所分配的 IP 地址的子网掩码、默认网关、DNS 服务器、租约期、续约时间等信息加上。

```
IP:ID = 0x3D30; Proto = UDP; Len: 328
IP:Version = 4 (0x4)
IP:Header Length = 20 (0x14)
```

```
IP:Service Type = 0 (0x0)
IP:Precedence = Routine
IP:...0.... = Normal Delay
IP:....0... = Normal Throughput
IP:.....0.. = Normal Reliability
IP:Total Length = 328 (0x148)
IP:Identification = 15664 (0x3D30)
IP:Flags Summary = 0 (0x0)
IP:.......0 = Last fragment in datagram
IP:......0. = May fragment datagram if necessary
IP:Fragment Offset = 0 (0x0) bytes
IP:Time to Live = 128 (0x80)
IP:Protocol = UDP - User Datagram
IP:Checksum = 0x2EA8
IP:Source Address = 157.54.48.151
IP:Destination Address = 255.255.255.255
IP:Data:Number of data bytes remaining = 308 (0x0134)

DHCP:ACK                        (xid=21274A1D)
DHCP:Op Code                   (op)      = 2 (0x2)
DHCP:Hardware Type           (htype)   = 1 (0x1) 10Mb Ethernet
DHCP:Hardware Address Length (hlen) = 6 (0x6)
DHCP:Hops                      (hops)    = 0 (0x0)
DHCP:Transaction ID        (xid)      = 556223005 (0x21274A1D)
DHCP:Seconds                  (secs)    = 0 (0x0)
DHCP:Flags                    (flags)   = 1 (0x1)
DHCP:1............... = Broadcast
DHCP:Client IP Address (ciaddr) = 0.0.0.0
DHCP:Your     IP Address (yiaddr) = 157.54.50.5
DHCP:Server IP Address (siaddr) = 157.54.48.151
DHCP:Relay    IP Address (giaddr) = 0.0.0.0
DHCP:Client Ethernet Address (chaddr) = 08002B2ED85E
DHCP:Server Host Name    (sname)   = JUMBO-WS
DHCP:Boot File Name       (file)      = <Blank>
DHCP:Magic Cookie = [OK]
DHCP:Option Field           (options)
DHCP:DHCP Message Type          = DHCP ACK
DHCP:Renewal Time Value (T1) = 8 Days,    0:00:00
DHCP:Rebinding Time Value (T2) = 14 Days,    0:00:00
DHCP:IP Address Lease Time    = 16 Days,    0:00:00
DHCP:Server Identifier          = 157.54.48.151
DHCP:Subnet Mask                  = 255.255.240.0
DHCP:Router                        = 157.54.48.1
DHCP:NetBIOS Name Service    = 157.54.16.154
DHCP:NetBIOS Node Type          = (Length: 1) 04
DHCP:End of this option field
```

说明 客户端在收到服务器返回的 DHCP-ACK 确认报文后，会以广播的方式发送免费 ARP 报文（该报文中，源 IP 地址和目标 IP 地址都是本机 IP 地址，源 MAC 地址是本机 MAC 地址，目的 MAC 地址是广播 MAC 地址），探测是否有主机使用服务器分配的 IP 地址，如果在规定的时间内没有收到回应，客户端才使用此地址。否则，客户端会发送 DHCP DECLINE 报文给 DHCP 服务器，并重新申请 IP 地址。

如果网络中存在多个 DHCP 服务器，除 DHCP 客户端选中的服务器外，其他 DHCP 服务器中本次未分配出的 IP 地址仍可分配给其他客户端。

5.1.4 DHCP 服务 IP 地址租约更新原理

DHCP 服务器按照如下优先次序为客户端选择 IP 地址。

① DHCP 服务器的数据库中与客户端 MAC 地址静态绑定的 IP 地址。

② 客户端以前曾经使用过的 IP 地址，即客户端发送的 DHCP DISCOVER 报文中请求 IP 地址选项的地址。

③ 在 DHCP 地址池中，在顺序查找可供分配的 IP 地址中，最先找到的 IP 地址。

④ 如果在 DHCP 地址池中未找到可供分配的 IP 地址，则依次查询超过租期、发生冲突的 IP 地址，如果找到可用的 IP 地址，则进行分配，否则报告错误。

DHCP 服务器分配给客户端的 IP 地址都是有一定的租约期限的，当租约期满后 DHCP 服务器又会收回原来分配的这个 IP 地址。如果 DHCP 客户端希望继续使用该地址，则需要向 DHCP 服务器提出更新 IP 地址租约的申请，也就是前面所说到的"续约"。IP 地址租约更新，或者 IP 地址续约也就是更新服务器端对 IP 地址租约信息，使其恢复为初始状态。

DHCP 客户端申请续约的步骤如下。

① 在 DHCP 客户端的 IP 地址租约期限达到 **1/2** 时，DHCP 客户端会向为它分配 IP 地址的 DHCP 服务器**以单播方式**发送 DHCP REQUEST 请求报文，以期进行 IP 租约的更新。

② 如果 DHCP 服务器同意续约，则 DHCP 服务器向客户端**以单播方式**返回 DHCP ACK 报文，通知 DHCP 客户端已经获得新 IP 租约，可以继续使用此 IP 地址；相反，如果 DHCP 服务器不同意续约，则 DHCP 服务器**以单播方式**返回 DHCP NAK 报文，通知 DHCP 客户端不能获得新的租约，此 IP 地址不可以再分配给该客户端。

③ 如果上面的续约申请失败，则 DHCP 客户端还会在租约期限达到 **7/8** 时，再次**以单播方式**发送 DHCP REQUEST 请求报文进行续约。DHCP 服务器的处理方式同上，不再赘述。

如果第二次续约请求还是失败，则原来租约的 IP 地址将被释放。

说明 不管是在第一次分配，还是续约分配 IP 地址前，为防止 IP 地址重复分配导致地址冲突，DHCP 服务器都需要先对要分配的 IP 地址进行探测。地址探测是通过 Ping 命令实现的，检测是否能在指定时间内得到 Ping 应答。如果没有得到应答，则继续发送 Ping 报文，直到发送 Ping 包的数量达到最大值。如果仍然超时，则可以认为这个 IP 地址的网段内没有设备使用该 IP 地址，从而确保客户端分得的 IP 地址是唯一的。DHCP 客户端在获得了一个 IP 地址以后，也会发送一个免费 ARP 请求探测网络中是否还有其他主机使用 IP 地址，来避免由于 DHCP 服务器地址池重叠而引发的 IP 冲突。

5.1.5 DHCP 中继代理服务

因为在 DHCP 客户端初次从 DHCP 服务器获取 IP 地址的过程中，所有从 DHCP 客

户端发出的请求报文和所有由 DHCP 服务器返回的应答报文均是**以广播方式**（目的地址为 255.255.255.255）进行发送的，所以 DHCP 服务只适用于 DHCP 客户端和 DHCP 服务器处于同一个子网（也就是 DHCP 服务器有至少有一个端口是与 DHCP 客户端所在子网是直接连接的）的情况，因为广播包是不能穿越子网的。

基于 DHCP 服务的以上限制，如果 DHCP 客户端与 DHCP 服务器之间隔了路由设备，不在同一子网就不能直接通过这台 DHCP 服务器获取 IP 地址，即使 DHCP 服务器上已配置了对应的地址池。这也就意味着，如果想要让多个子网中的主机进行动态 IP 地址分配，就需要在网络中的所有子网中都设置一个 DHCP 服务器。这显然是很不经济的，也是没有必要的。

幸好，DHCP 中继功能可以很好地解决 DHCP 服务的以上难题。通过 DHCP 中继代理服务，与 DHCP 服务器不在同一子网的 DHCP 客户端可以通过 DHCP 中继代理（通常也是由路由器，或三层交换机设备担当，但需要开启 DHCP 中继功能）与位于其他网段的 DHCP 服务器通信，最终使 DHCP 客户端获取到从 DHCP 服务器上分配而来的 IP 地址。此时的 DHCP 中继代理就位于 DHCP 客户端和 DHCP 服务器之间，负责广播 DHCP 报文的转发，如图 5-4 所示。

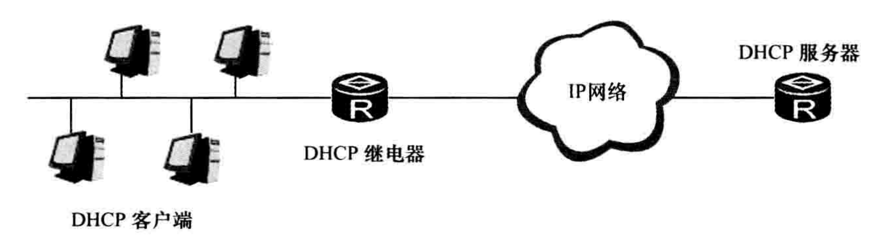


图 5-4　DHCP 中继代理的典型应用示例

很显然，DHCP 中继代理必须至少有一个端口连接了 DHCP 客户端所在子网，另一端又直接连接了 DHCP 服务器的一个端口所在子网。当然，一个 DHCP 中继代理可以同时连接多个子网，作为多个 DHCP 客户端子网的中继代理。这样，多个子网上的 DHCP 客户端又可以使用同一个 DHCP 服务器来进行 IP 地址的自动分配了，既节省了成本，又便于进行集中管理。

1. DHCP 中继代理简介

Option 82 是 DHCP 报文中的中继代理信息选项（Relay Agent Information Option），该选项记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 选项的 DHCP 服务器还可以根据该选项的信息制订 IP 地址和其他参数的分配策略，提供更加灵活的地址分配方式。

在整个 Option 82 选项中最多可以包含 255 个子选项，且至少要定义一个子选项。目前的设备主要只支持两个子选项：sub-option 1（Circuit ID，电路 ID 子选项）和 sub-option 2（Remote ID，远程 ID 子选项）。由于 RFC 3046 对于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。目前，设备作为 DHCP 中继设备都支持 Option 82 子选项的扩展填充格式。

sub-option 1 和 sub-option 2 两个子选项的格式分别如图 5-5 和图 5-6 所示，固定字段（相当于子选项头）括号中的内容为该字段的固定取值。sub-option 1 子选项中的内容是

接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号（对应“VLAN ID”字段，占 2 字节）以及端口索引（端口索引的取值为端口物理编号减 1，对应“Port Index”字段，占 2 字节）。sub-option 2 子选项的内容是接收到 DHCP 客户端请求报文的 DHCP 中继设备的 MAC 地址（对应“MAC Address”字段，占 6 字节）。

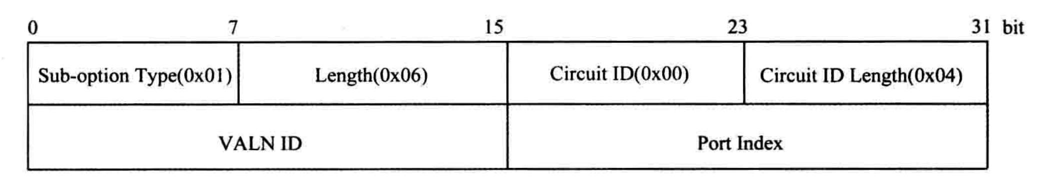


图 5-5　sub-option 1 子选项格式及默认填充

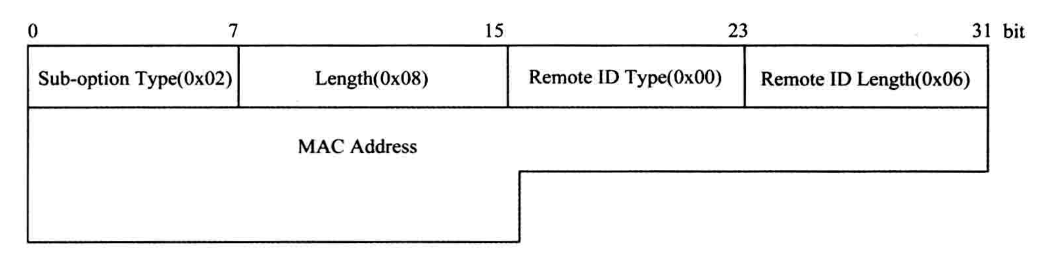


图 5-6　sub-option 2 子选项格式及默认填充

2. 通过 DHCP 中继代理动态 IP 地址分配原理

DHCP 客户端通过 DHCP 中继代理服务从 DHCP 服务器动态获取 IP 地址的过程与 5.1.3 小节中介绍的不通过 DHCP 中继代理，直接从 DHCP 服务器动态获取 IP 地址的过程基本相同，都要经历发现、提供、选择和确认 4 个阶段。所用的到报文也对应是 DHCP DISCOVER、DHCP OFFER、DHCP REQUEST、DHCP ACK，只是在这里 DHCP 中继代理需要起到一具中介代理的角色，负责转发 DHCP 客户端与 DHCP 服务器之间交互的这些报文，基本流程如图 5-7 所示。

说明 在此流程中，DHCP 客户端发送的请求报文有两种，分别为 DHCP DISCOVER 报文和 DHCP REQUEST 报文。由于不同厂商生产的 DHCP 服务器设备对请求报文的处理机制不同，有些设备处理 DHCP DISCOVER 报文中的 Option 82 信息，而有些处理 DHCP REQUEST 报文中的 Option 82 信息，因此 DHCP 中继设备将在这两种报文中都添加 Option 82 选项。

这里将只介绍 DHCP 中继支持 Option 82 时的工作机制，具体如下。

① DHCP 客户端**以广播方式**（因为不知中继代理设备的 IP 地址）向本网段发送 DHCP DISCOVER 或 DHCP REQUEST 请求报文。此时只有网络中的 DHCP 中继代理设备会接收该 DHCP 请求报文（假设本网段中没有 DHCP 服务器）。

② DHCP 中继代理设备在收到 DHCP 客户端发来的 DHCP DISCOVER 或 DHCP REQUEST 请求报文后，将检查报文中是否已有 Option 82 选项，主要是以上介绍的 sub-option 1 子选项和 sub-option 2 子选项。

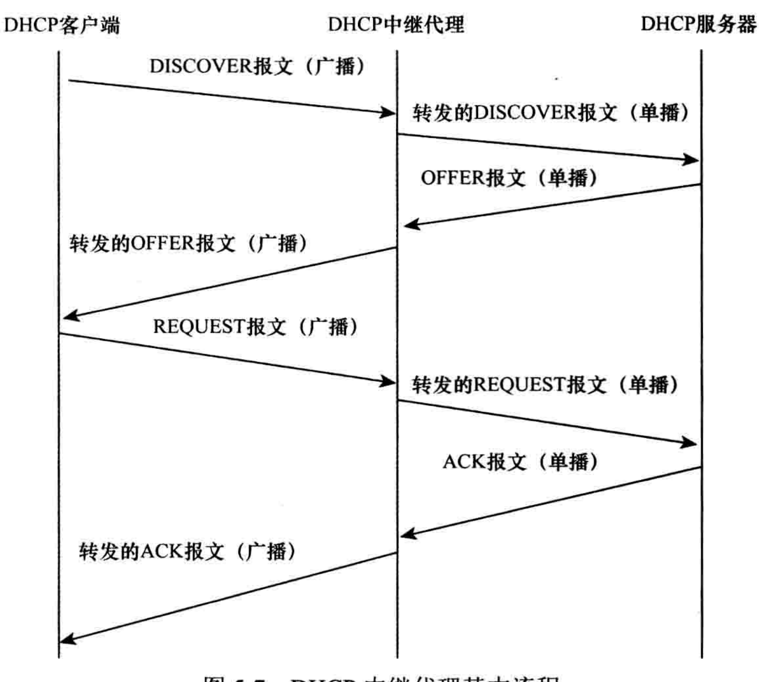


图 5-7 DHCP 中继代理基本流程

如果请求报文中已有 Option 82，DHCP 中继代理设备会按照配置的策略对该报文进行处理（丢弃或者用中继设备本身的 Option 82 选项替代报文中原有的 Option 82 选项，或保持报文原有的 Option 82 选项）。同时，根据 Option 82 选项 sub-option 1 子选项中的 VLAN ID 和 Port Index 字段配置，找到为对应网段所分配的 DHCP 服务器地址，并将请求报文中的 giaddr 字段填充为 DHCP 中继代理设备的 IP 地址，然后将请求报文**以单播方式**（因为在中继代理设备中已配置好了对应的 DHCP 服务器地址）转发给指定的 DHCP 服务器。

如果请求报文中没有 Option 82 选项，则 DHCP 中继设备将 Option 82 选项添加到报文中后，根据 Option 82 选项 sub-option 1 子选项中的 VLAN ID 和 Port Index 字段配置，找到为对应网段所分配的 DHCP 服务器地址，并将报文中的 giaddr 字段填充为 DHCP 中继代理设备的 IP 地址，然后同样根据中继代理设备中为对应网段所配置的 DHCP 服务器地址**以单播方式**将请求报文转发给 DHCP 服务器。

③ DHCP 服务器在收到由 DHCP 中继代理设备转发的 DHCP DISCOVER 或 DHCP REQUEST 请求报文后，根据转发的请求报文中的 giaddr 字段值所对应的中继代理设备 IP 地址，以及在 Option 82 选项中 sub-option 2 子选项中的中继代理 MAC 地址**以单播方式**向 DHCP 中继代理返回对应的 DHCP OFFER 或者 DHCP ACK 应答报文。

④ DHCP 中继设备在收到 DHCP 服务器的应答报文后，将剥离报文中的 Option 82 信息，然后以**广播方式**将带有 DHCP 配置信息的对应应答报文转发给 DHCP 客户端，完成对客户端的 IP 地址动态分配。

在以上过程中，4 种 DHCP 报文中除 Option 82 选项和 giaddr 字段外，其他各字段

值均与 5.1.3 小节介绍的非中继方式动态分配 IP 地址过程中的四种报文所对应的字段值是一样的。

5.2 配置基于全局地址池的 DHCP 服务器

充当 DHCP 服务器是路由器的一项重要功能。当要把 AR G3 系列路由器配置为 DHCP 服务器时，需要首先创建 IP 地址池，从中选择合适的 IP 地址分配给 DHCP 客户端。

在 AR G3 系列路由器中，可以创建“全局地址池”（是在系统视图下全局配置的）和“接口地址池”（是在 DHCP 服务器连接 DHCP 客户端的对应接口视图下配置的）两种 IP 地址池（**同一网段的地址池仅可采用其中一种模式**）。基于全局地址池的 DHCP 服务器一般应用于 DHCP 服务器和 DHCP 客户端在不同网段的情况。而对于基于接口地址池的 DHCP 服务器，只有从对应接口上线的用户才可以从该地址池中分配地址，一般应用于 DHCP 服务器和 DHCP 客户端在同一网段的情况。本节先介绍全局地址池的配置，接口地址池的配置将在下节介绍。

5.2.1 基于全局地址池的 DHCP 服务器的配置任务

配置基于全局地址池的 DHCP 服务器时，从设备上所有接口上线的用户都可以选择对应地址池进行 IP 地址分配（**但与 DHCP 服务器接口不在同一网段的 DHCP 客户端需要通过 DHCP 中继来从 DHCP 服务器全局地址池中获取 IP 地址**）。它的基本配置思想就是，在系统视图下为各 DHCP 客户端所在网段配置对应网段的 IP 地址池（包括指定地址池所在网段，以及可选配置的排除地址、地址租用期、需静态绑定的 IP 地址、网关 IP 地址等信息），然后在 DHCP 服务器连接对应 DHCP 客户端的接口（**可以是物理接口，也可以是像 VLANIF、Eth-Trunk、以太网子接口等之类的逻辑接口，但必须是三层接口**）上使能基于全局地址的 DHCP 服务器功能，这样 DHCP 服务器就会自动选择对应的全局地址池为对应网段的 DHCP 客户端分配 IP 地址。

配置基于全局地址池的 DHCP 服务器所包括的配置任务如下。（**仅前面两项是必须配置的**，其他各项均有缺省配置，或者在对应网络环境中不需要配置，仅需要根据实际需要选择配置。）

① 配置全局地址池。

② 配置接口工作在全局地址池模式。

③（可选）配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务。

④（可选）配置全局地址池 DHCP 自定义选项。

因此部分涉及比较复杂的 DHCP Options 字段的许多选项类型，且一般情况下无需配置，故在此不做介绍。

⑤（可选）配置防止 IP 地址重复分配功能。

⑥（可选）配置 DHCP 数据保存功能。

⑦（可选）配置 DHCP 服务器信任 Option82 选项功能。

⑧（可选）配置 DHCP 服务器为 BOOTP 客户端分配 IP 地址。

在配置基于全局地址池的 DHCP 服务器之前，需完成以下任务。

① 保证 DHCP 客户端和设备之间链路正常，能够通信。

② 配置客户端的 DNS 服务器（根据实际需要，可选择配置）。

③ 配置客户端的 NetBIOS 服务器（根据实际需要，可选择配置）。

④ 配置设备到 DNS 服务器和 NetBIOS 服务器的路由（如果没有配置这两种服务器，则无需配置路由）。

⑤ 配置 DHCP 自定义选项（根据实际需要，可选择配置）。

5.2.2 配置全局地址池

这项配置任务包括创建全局地址池，然后配置包括地址范围、地址租期、要排除的 IP 地址以及要静态绑定的 IP 地址的全局地址池属性。具体如表 5-2 所示。

表 5-2　全局地址池的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ip pool** *ip-pool-name* 例如：[Huawei] **ip pool** global1	创建全局地址池，同时进入全局地址池视图。参数 *ip-pool-name* 用来指定所创建的地址池名称，不支持空格，1～64 个字符，可以设定为包含数字、字母和下划线“_”或“.”的组合 【说明】可以为不同网段的 DHCP 客户端创建**多个不同网段**的全局地址池，但多个地址池中的 IP 地址范围不能重叠或者交叉 缺省情况下，设备上没有创建任何全局地址池，可用 **undo ip pool** *ip-pool-name* 命令删除指定的全局地址池。但如果全局地址池的 IP 地址正在使用，不能删除该全局地址池
3	**network** *ip-address* [**mask** { *mask* | *mask-length* }] 例如：[Huawei] **ip pool** global1	配置全局地址池可动态分配的 IP 地址范围。命令中的参数说明如下 • *ip-address*：指定地址中的网络地址段，必须是一个网络 IP 地址，不能是主机 IP 地址和广播 IP 地址 • **mask** { *mask* | *mask-length* }：可选参数，指定 IP 地址池中 IP 地址对应的子网掩码（选择 *mask* 参数时）或者子网掩码长度（选择 *mask-length* 参数时），**但子网掩码长度不能小于 16**。如果不指定该参数时，则地址池中的 IP 地址使用对应的标准网络子网掩码（**仅可以是 B、C 类网络对应的子网掩码**） 【注意】**每个 IP 地址池只能配置一个网段**，该网段可配置为需求的任意网段。如果系统需要多网段 IP 地址，则需要配置多个全局地址池，**但不同地址池中的 IP 地址范围不能重叠或者交叉，且所配置的地址池范围不能大于 64 K 个（1 K=1 024）** 缺省情况下，系统未配置全局地址池下动态分配的 IP 地址范围，可用 **undo network** 命令删除所有配置的全局地址池中的地址范围

（续表）

步骤	命令	说明
4	**lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } 例如：[Huawei-ip-pool-global1] **network** 10.10.10.0 **mask** 24	（可选）配置地址池中的 IP 地址租用期。命令中的参数和选项说明如下 • **day** *day*：指定客户端租用 IP 地址的期限，取值范围为 0～999 的整数，缺省值是 1 • **hour** *hour*：二选一可选参数，指定客户端租用 IP 地址的小时数，取值范围是 0～23 的整数，缺省值是 0 • **minute** *minute*：可选参数，指定客户端租用 IP 地址的分钟数，取值范围是 0～59 的整数，缺省值是 0 • **unlimited**：二选一可选选项，指定客户端可以无限期租用所分配的 IP 地址 【说明】DHCP 服务器可以为不同的全局地址池指定不同的地址租用限。通常在 DHCP 客户端启动或 IP 地址租用期达到一半时，DHCP 客户端会自动向 DHCP 服务器申请，以完成 IP 续租。如果此 IP 地址可继续分配给该客户端使用，则 DHCP 服务器通知 DHCP 客户端获得新 IP 租用；如果此 IP 地址不可以再分配给该客户端，则 DHCP 服务器通知 DHCP 客户端不能获得新的租用，该客户端需要申请其他 IP 地址 缺省情况下，客户端租用 IP 地址的期限为 1 天，可用 **undo lease** 命令恢复地址池缺省租用期配置
5	**excluded-ip-address** *start-ip-address* [*end-ip-address*] 例如：[Huawei-ip-pool-global1] **excluded-ip-address** 10.10.10.10 10.10.10.20	（可选）配置地址池中不参与自动分配的 IP 地址，也即要排除分配的 IP 地址。因为地址池中有些 IP 地址因特殊用途需要保留，有些 IP 地址被长期固定分配给某些特定主机（例如 DNS 服务器、WWW 服务器、其他关键设备接口等，**但是路由器接口 IP 地址缺省就已排除，不用再单独排除**）后就不能再进行自动分配。命令中的参数说明如下 • *start-ip-address*：指定要排除的 IP 地址段的起始 IP 地址 • *end-ip-address*：可选参数，指定要排除的 IP 地址段的结束 IP 地址，应与 *start-ip-address* 在同一网段，并且不能小于 *start-ip-address*。如果不指定该参数，表示只有参数 *start-ip-address* 指定的这个 IP 地址被排除 【说明】被排除的 IP 地址或 IP 地址段必须在本地址池范围内。多次执行此命令可以排除多个不参与自动分配的 IP 地址或 IP 地址段 缺省情况下，地址池中所有 IP 地址都参与自动分配，可用 **undo excluded-ip-address** *start-ip-address* [*end-ip-address*]命令删除指定的原来被排除的 IP 地址范围
6	**gateway-list** *ip-address* &<1-8> 例如：[Huawei-ip-pool-global1] **gateway-list** 10.10.10.1	配置到达 DHCP 客户端的网关地址，也就是 DHCP 服务器直接连接 DHCP 客户端，或者 DHCP 中继的接口的 IP 地址。参数 *ip-address* &<1-8>用来为对应地址池中 DHCP 客户端指定最多 8 个（**以空格分隔**）网关 IP 地址（**必须与地址池中的 IP 地址在同一网段**） 缺省情况下，没有配置出口网关地址，可用 **undo gateway-list** { *ip-address* | **all** }命令删除对应地址池中指定的或所有的网关配置

（续表）

步骤	命令	说明
7	**static-bind ip-address** *ip-address* **mac-address** *mac-address* 例如：[Huawei-ip-pool-global1] **static-bind ip-address** 10.10.10.10 **mac-address** dcd2-fc96-e4c0	（可选）采用静态地址绑定方式将全局地址池中的 IP 地址与 DHCP 客户端的 MAC 地址绑定。相当于静态为某客户端分配 IP 地址。当有用户（如某服务器）需要固定的 IP 地址时，可以将地址池中尚未分配的 IP 地址与用户的 MAC 地址绑定，**这样这个 IP 地址就只会分配给对固定的 DHCP 客户端**。命令中的参数说明如下 • *ip-address*：指定要绑定的 IP 地址，必须是当前全局地址池中的合法 IP 地址 • *mac-address*：指定以上 IP 地址要绑定的用户 MAC 地址 【说明】DHCP 服务器选择分配为客户端的 IP 地址时，优先选择与客户端 MAC 地址绑定的 IP 地址。地址池中已绑定 MAC 地址的 IP 地址不在租期管理范围内（**也就是不受前面配置的租期限制，永远有效**），当 IP 地址绑定的用户正在使用此 IP 地址时，管理员不能在地址池中删除其配置 缺省情况下，全局地址池下的 IP 地址没有与任何 MAC 地址绑定，可用 **undo static-bind** [**ip-address** *ip-address* | **mac-address** *mac-address*] 命令删除全局地址池下指定的 IP 地址与 MAC 地址的绑定关系
8	**next-server** *ip-address* 例如：[Huawei-ip-pool-global1] **next-server** 10.1.2.2	（可选）配置客户端自动获取 IP 地址后下一步使用的其他网络服务器（**不是用来提供 IP 地址自动分配的 DHCP 服务器**）地址，参数 *ip-address* 用来指定下一步要使用的其他网络服务器 IP 地址 【说明】DHCP 服务器在给客户端分配 IP 地址的同时，也可以为客户端分配提供网络服务的服务器 IP 地址。例如，某些类似 IP Phone 等客户端，在自动获取 IP 地址后，还需要其他配置参数才能正常工作。执行本命令配置客户端自动获取 IP 地址后下一步使用的服务器地址，客户端在自动获取 IP 地址后，会向指定的服务器请求配置信息。**但每个 IP 地址池只能配置一个提供网络服务的服务器 IP 地址**，该命令可执行多次，但最后一次配置的 IP 地址有效 缺省情况下，设备未配置客户端自动获取 IP 地址后下一步使用的服务器地址，可用 **undo next-server** 命令删除已经配置的客户端自动获取 IP 地址后下一步使用的服务器地址
9	**vpn-instance** *vpn-instance-name* 例如：[Huawei-ip-pool-global1] **vpn-instance** huawei	（可选）配置地址池下的 VPN 实例，仅在 VPN 实例下配置 DHCP 服务器时才需要进行。参数 *vpn-instance-name* 用来指定以上创建的全局地址池所应用的 VPN 实例名称（必须在此之前先创建对应的 VPN 实例），1～31 个字符，区分大小写，不支持空格，可以设定为包含数字、字母和下划线“_”或“.”的组合 缺省情况下，地址池下没有配置 VPN 实例，可用 **undo vpn-instance** 命令恢复缺省配置

（续表）

步骤	命令	说明
10	**lock** 例如：[Huawei-ip-pool-global1] **lock**	（可选）锁定客户端正在使用的 IP 地址池。当 DHCP 服务器进行网络重新部署时，需要将原 DHCP 服务器上的地址池转移到另外一台现有网络中的 DHCP 服务器设备。为了不影响已经从全局地址池申请了 IP 地址的用户正常工作，需要使用 **lock** 命令锁定该地址池，**使 IP 地址池锁定后不能继续为客户端分配 IP 地址。**当地址池转移后，新用户上线时会向新的地址池申请 IP 地址 缺省情况下，系统未锁定 IP 地址池，可用 **undo lock** 命令恢复缺省配置

5.2.3 配置连接客户端的接口工作在全局地址池模式

配置了全局地址池后，还需要配置连接 DHCP 客户端或者 DHCP 中继设备的对应 DHCP 服务器接口启用全地址池的 DHCP 服务器功能。这项配置任务主要包括 3 个基本方面的配置：一是全局使能路由器的 DHCP 服务器功能，使它担当 DHCP 服务器；二是为 DHCP 服务器连接 DHCP 客户端或 DHCP 中继设备的各个接口（可以是物理接口，也可以是像 VLANIF、Eth-Trunk、以太网子接口和 Eth-Trunk 子接口这样的逻辑接口）上配置对应网段的 IP 地址配置，使它们成为对应网段 DHCP 客户端的出口网关 IP 地址；三是使能这些接口采用全局地址池的 DHCP 服务器功能。具体配置很简单，如表 5-3 所示。

表 5-3　　连接客户端的接口工作在全局地址池模式的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp enable** 例如：[Huawei] **dhcp enable**	使能路由器的 DHCP 服务功能，也就是打开 DHCP 服务开关 缺省情况下，**系统未使能 DHCP 服务功能**，可用 **undo dhcp enable** 命令去使能 DHCP 功能 **【注意】dhcp enable 命令是 DHCP 相关功能的总开关，**DHCP 中继、DHCP Snooping、DHCP 服务器等功能都要在执行 **dhcp enable** 命令使能 DHCP 功能后才会生效。**执行 undo dhcp enable 命令后，所有的 DHCP 功能都将失效** 设备作为 DHCP 服务器时，如果使能了 STP 功能，可能会造成地址分配较慢。STP 功能缺省处于使能状态，如果确认不需要使能 STP 功能，可以执行 **undo stp enable 命令**去使能 STP 功能
3	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要使能接口采用全局地址池的 DHCP 服务器功能的路由器接口（可以是三层 GE 接口及其子接口、VLANIF 接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口）

（续表）

步骤	命令	说明
4	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-GigabitEthernet1/0/0] **ip address** 10.10.10.2 24	配置以上三层接口的 IP 地址。命令中的参数说明如下 • *ip-address*：指定接口的 IP 地址，必须是一个主机 IP 地址，不能是网络 IP 地址和广播 IP 地址，**但必须与对应地址池中的 IP 地址在同一网段** • **mask** { *mask* | *mask-length* }：指定以上接口 IP 地址对应的子网掩码（选择 *mask* 参数时）或者子网掩码长度（选择 *mask-length* 参数时） 【说明】配置了接口的 IP 地址后，此接口下的用户申请 IP 地址时： • 如果 DHCP 客户端和作为 DHCP 服务器的路由器处于同一个网段，不需要中继进行转发时，路由器会选择与此接口的 IP 地址在同一个网段的地址池来分配 IP 地址。**如果该接口未配置 IP 地址**，或者没有和接口地址在相同网段的地址池，**用户无法上线** • 如果 DHCP 客户端和作为 DHCP 服务器的路由器处于不同网段，需要由 DHCP 中继设备进行转发时，DHCP 服务器解析收到的 DHCP 请求报文中 giaddr 字段指定的 IP 地址，选择与此 IP 地址在同一个网段的地址池来进行 IP 地址分配，如果该 IP 地址匹配不到相应的地址池，则用户上线失败 缺省情况下，在接口上没有配置 IP 地址，可用 **undo ip address** [*ip-address* { *mask* | *mask-length* } 命令删除接口上配置的指定 IP 地址
5	**dhcp select global** 例如：[Huawei-GigabitEthernet1/0/0] **dhcp select global**	使能以上接口采用全局地址池的 DHCP 服务器功能，使从该接口上线的用户可以从全局地址池中获取 IP 地址等配置信息 缺省情况下，接口采用全局地址池的 DHCP 服务器功能处于未使能状态，可用 **undo dhcp select global** 命令去使能以上接口采用全局地址池的 DHCP 服务器功能

5.2.4　配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务

为了保证 DHCP 客户端的正常通信，DHCP 服务器在给客户端分配 IP 地址的同时，可能需指定 DNS 服务器的配置信息和 NetBIOS 的配置信息（**主要是当网络中采用了 DNS 服务器或者 WINS 服务器进行名称解析时才配置**）。用户如果不知道运营商分配的这些配置信息，可以采用动态配置的方式自动把运营商分配的 DNS 配置信息和 NetBIOS 配置信息分配给 DHCP 客户端。当地址池中同时配置了静态、动态 DNS、NetBIOS 等信息时，以静态配置优先。**但本项配置任务均为可选配置，根据实际需要选择配置。**

说明　当 DHCP 客户端使用 NetBIOS 协议进行名称解析时（即不是采用 DNS 协议进行名称解析时，如工作组网络中），需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为 4 种。

① b 类节点（b-node）："b" 代表广播（broadcast），即此类节点采用广播的方式获

取映射关系，如在广播式的以太网中可采用这种类型，但效率较低。

②p 类节点（p-node）："p" 代表端到端（peer-to-peer），即此类节点采用与 NetBIOS 服务器（如 Windows 系统中的 WINS 服务器）通信的方式获取映射关系。在网络中配置了 NetBIOS 服务器时通常采用这种方式，效率更高。

③ m 类节点（m-node）："m" 代表混合（mixed），是具有部分广播特性的 p 类节点，先使用 b 节点方式，后使用 p 节点方式，比单一的 b 节点类型或者 p 节点类型更加可靠。

④ h 类节点（h-node）："h" 代表混合（hybrid），是具备"端对端"通信机制的 b 类节点，先使用 p 节点方式，后使用 b 节点方式，比单一的 p 节点类型或者 b 节点类型更加可靠。

DHCP 客户端的 DNS 服务和 NetBIOS 服务的具体配置步骤如表 5-4 所示。

表 5-4　DHCP 客户端的 DNS 服务和 NetBIOS 服务的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ip pool** *ip-pool-name* 例如：[Huawei] **ip pool** global1	进入前面创建的全局地址池
3	**import all** 例如：[Huawei-ip-pool-global] **import all**	（可选）动态配置 DHCP 客户端使用的 DNS 配置信息和 NetBIOS 配置信息，可以自动把运营商分配的 DNS 和 NetBIOS 服务器的配置信息分配给 DHCP 客户端 【说明】DNS 和 NetBIOS 服务器的动态配置与下一步的静态配置可以同时配置，以静态配置优先。动态配置 DNS 和 NetBIOS 信息后，如果用户希望静态指定 DNS 服务器和 NetBIOS 服务器的 IP 地址，则需要选择下面各步进行静态配置，否则无需进行 DNS 和 NetBIOS 信息的静态配置 缺省情况下，全局地址池下动态获取 DNS 和 NetBIOS 服务器配置信息的功能处于未使能状态，可用 **undo import all** 命令去使能全局地址池下动态获取 DNS 和 NetBIOS 服务器的配置信息
4	**domain-name** *domain-name* 例如：[Huawei-ip-pool-pool1] **domain-name** huawei.com	（可选）配置为 DHCP 客户端分配的域名后缀。参数 *domain-name* 用来指定为 DHCP 客户端分配的域名后缀，1～50 个字符，不支持空格，可以设定为包含数字、字母和下划线"_"或"."的组合 【说明】通过本命令可以在每个全局地址池上指定客户端使用的域名。在给客户端分配 IP 地址的同时，也将域名后缀发送给客户端 缺省情况下，系统未配置为 DHCP 客户端分配的域名后缀，可用 **undo domain-name** 命令删除为对应地址池中的 DHCP 客户端配置的域名后缀
5	**dns-list** *ip-address* &<1-8> 例如：[Huawei-ip-pool-global1] **dns-list** 10.10.10.10	（可选）配置 DHCP 客户端使用的 DNS 服务器的 IP 地址。参数 *ip-address* &<1-8>用来为 DHCP 客户端分配最多 8 个 DNS 服务器 IP 地址。其中第一个分配给客户端作为主用地址，其他 7 个作为备用地址（还可用于对流量进行负载分担和提高网络的可靠性）

（续表）

步骤	命令	说明
5	**dns-list** *ip-address* <1-8> 例如：[Huawei-ip-pool-global1] **dns-list** 10.10.10.10	【说明】当用户主机以域名方式访问网络服务器时，需要先将域名请求发送至 DNS 服务器，DNS 服务器将待访问的域名解析为 IP 地址并返回给主机后，主机才可以进行正常通信。为了保证 DHCP 客户端可以正确接入网络，DHCP 服务器需要在全局地址池上指定 DNS 服务器的 IP 地址，DHCP 服务器在为客户端分配 IP 地址的同时也指定了 DNS 服务器 IP 地址 缺省情况下，全局地址池下未配置 DNS 服务器地址，可用 **undo dns-list** { *ip-address* | **all** }命令删除全局地址池下指定的或者全部 DNS 服务器 IP 地址
6	**nbns-list** *ip-address* <1-8> 例如：[Huawei-ip-pool-global1] **nbns-list** 1.1.1.1	（可选）配置 DHCP 客户端的 NetBIOS 服务器地址。参数 *ip-address* <1-8>用来为 DHCP 客户端分配最多 8 个 NetBIOS 服务器 IP 地址。其中第一个分配给客户端的作为主用地址，其他 7 个作为备用地址（还可用于对流量进行负载分担和提高网络的可靠性） 【说明】当用户主机之间通信时，需要借助 NetBIOS 服务器将待访问的 NetBIOS 主机名解析为 IP 地址后进行通信。为了使主机能正常通信，可使用本命令配置 DHCP 服务器端当前全局地址池的 NetBIOS 服务器地址。当 DHCP 服务器给用户分配 IP 地址时，也一并将 NetBIOS 服务器地址分配给用户 缺省情况下，全局地址池中没有配置 NetBIOS 服务器，可用 **undo nbns-list** { *ip-address* | **all** }命令删除全局地址池下指定的或者全部 NetBIOS 服务器 IP 地址
7	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } 例如：[Huawei-ip-pool-global1] **netbios-type b-node**	（可选）配置 DHCP 客户端的 NetBIOS 节点类型。命令中的选项说明如下。 • **b-node**：多选一选项，指定 DHCP 客户端为广播模式节点（broadcast），采用广播模式获取主机名和 IP 地址之间的映射 • **h-node**：多选一选项，指定 DHCP 客户端为混合 h 模式节点（hybrid），是具备“端到端”通信机制的 b 类节点 • **m-node**：多选一选项，指定 DHCP 客户端为混合 m 模式节点（mixed），是具有部分广播特性的 p 类节点 • **p-node**：多选一选项，指定 DHCP 客户端端到端模式节点（peer-to-peer），采用与 NetBIOS 服务器通信的方式来获取映射关系 【说明】DHCP 客户端在使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系，使用本命令可配置全局地址池客户端的 NetBIOS 节点类型。DHCP 服务器在给客户端分配 IP 地址的同时，也将 NetBIOS 节点类型发送给客户端 缺省情况下，不指定客户端的 NetBIOS 节点类型，可用 **undo netbios-type** 命令恢复缺省配置

5.2.5 配置防止 IP 地址重复分配功能

为防止 IP 地址的重复分配而导致地址冲突，DHCP 服务器在为客户端分配 IP 地址

前，需要先通过 Ping 功能对该地址进行探测。如果在最长等待 Ping 响应的时间内没有得到应答，则继续发送 Ping 报文，直到发送 Ping 报文数量达到最大值，如果仍然没有收到应答，则认为本网段内没有设备使用该 IP 地址，从而确保分配给 DHCP 客户端的 IP 地址是唯一的。

为了使 DHCP 服务器对重复 IP 地址探测的时间不至于过长，可以配置最大 Ping 报文发送数量和最长探测时间。建议用户配置的总探测时间（发送 Ping 报文的最大数量×发送 Ping 报文的最长等待响应时间）小于 8 s。但因为本项配置任务中的两个配置命令都有缺省值，故为可选配置任务，可根据实际需要选择修改缺省值。

本项配置任务的具体配置方法很简单，就是在系统视图下使用 **dhcp server ping** { **packet** *number* | **timeout** *milliseconds* } *命令配置路由器发送 Ping 报文的最大数量和最长等待回应时间。命令中的参数说明如下。

① **packet** *number*：可多选参数，指定发送 Ping 报文的最大数目，取值范围为 0～10 的整数，取值为 0 表示不进行 ping 操作。

② **timeout** *milliseconds*：可多选参数，指定每个 Ping 报文的最长等待回应时间，取值范围为（0～10 000）的整数毫秒。

缺省情况下，DHCP 服务器发送 ping 报文数量为 0，最长等待回应时间 500 ms，可用 **undo dhcp server ping** { **packet** | **timeout** }命令恢复系统设定的缺省值。

【示例】配置 DHCP 服务器为探测 IP 地址冲突而发送的 Ping 报文最大次数为 10 次，每次等待的最长响应时间为 100 ms。

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server ping packet 10 timeout 100
```

5.2.6 配置 DHCP 数据保存功能

当路由器作为 DHCP 服务器使用时，用户可以启用 DHCP 数据保存功能，定时将地址信息保存到存储设备中（是指保存在本地 Flash 存储设备中），这样当设备发生故障时可以从存储设备中及时恢复数据。**本配置任务也为可选配置任务，可根据实际需要选择配置**。具体的配置步骤如表 5-5 所示。

表 5-5　DHCP 数据保存功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp server database enable** 例如：[Huawei]**dhcp server database enable**	使能 DHCP 数据保存到 Flash 存储设备的功能 缺省情况下，未使能 DHCP 数据保存到 Flash 存储设备的功能。执行本命令后，系统将生成 lease.txt 和 conflict.txt 两个文件（**由于 lease.txt 和 conflict.txt 这两个文件会被定期覆盖，建议用户在必要时将生成的文件备份到其他位置**），存放在 Flash 存储设备中的 DHCP 文件夹中，分别保存正常的地址租借信息和地址冲突信息，可用 **undo dhcp server database enable** 命令去使能 DHCP 数据保存到 Flash 的功能

（续表）

步骤	命令	说明
3	**dhcp server database write-delay** *interval* 例如：[Huawei] **dhcp server database write-delay** 600	配置数据保存时间间隔，取值范围为 300～86 400 s，取整数 缺省情况下，每隔 300 s 保存一次当前的 DHCP 数据，并覆盖之前的数据文件，可用 **undo dhcp server database write-delay** 命令恢复数据保存时间间隔为缺省值
4	**dhcp server database recover** 例如：[Huawei] **dhcp server database recover**	（可选）使能 DHCP 数据恢复功能，使系统重启时将从 Flash 存储设备的文件中恢复 DHCP 数据。**仅当需要恢复 DHCP 服务器数据时才进行操作** 缺省情况下，没有使能 DHCP 数据恢复功能，可用 **undo dhcp server database recover** 命令去使能 DHCP 数据恢复功能

5.2.7　配置 DHCP 服务器信任 Option82 选项功能

信任 Option82 选项（即 DHCP 中继代理信息选项）功能主要是为了使 DHCP 服务器在收到带有 Option82 选项，但是报文中的 giaddr 字段值却为 0.0.0.0（表示没有经过 DHCP 中继）的 DHCP 报文时，继续对报文进行处理，而不是丢弃。这主是要由于在 DHCP 客户端连接的交换机上开启了 DHCP 82 选项功能，使得 DHCP 客户端发出的 DHCP 请求报文在经过该交换机后自动插入 82 选项，但又因为确实没有经过 DHCP 中继设备，所以 giaddr 字段值为 0.0.0.0。

本项配置任务的配置很简单，仅需在系统视图下使用 **dhcp server trust option82** 命令使能 DHCP Server 信任 Option82 选项功能即可。缺省情况下，系统信任 Option82 选项功能处于使能状态，可用 **undo dhcp server trust option82** 命令去使能 DHCP Server 信任 Option82 选项功能。

5.2.8　配置 DHCP 服务器为 BOOTP 客户端分配 IP 地址

如果 DHCP 服务器所在的网络中存在 BOOTP 客户端（如无盘工作站），在设备作为 DHCP 服务器使用时就可以为 BOOTP 客户端分配 IP 地址。具体配置步骤也很简单，如表 5-6 所示。

表 5-6　　DHCP 服务器为 BOOTP 客户端分配 IP 地址的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp server bootp** 例如：[Huawei] **dhcp server bootp**	使能 DHCP 服务器应答 BOOTP 请求的功能 缺省情况下，DHCP 服务器使能了应答 BOOTP 请求的功能，可用 **undo dhcp server bootp** 命令去使能 DHCP 服务器应答 BOOTP 请求的功能
3	**dhcp server bootp automatic** 例如：[Huawei]**dhcp server bootp automatic**	使能 DHCP 服务器为 BOOTP 客户端分配地址的功能。当 BOOTP 客户端需要从服务器端获取绑定的 IP 地址、DNS 服务器、网关地址等信息时，需要通过本命令开启 DHCP 服务器为 BOOTP 客户端动态分配地址的功能 缺省情况下，DHCP 服务器为 BOOTP 客户端分配地址的功能处于未使能状态，可用 **undo dhcp server bootp automatic** 命令去使能 DHCP 服务器为 BOOTP 客户端分配地址的功能

5.2.9 基于全局地址池的 DHCP 服务器的配置示例

本示例的基本网络结构如图 5-8 所示，某企业有两个处于同一网络内的办公室，为了节省资源，两个办公室内的主机由 Router 作为 DHCP 服务器统一分配 IP 地址。

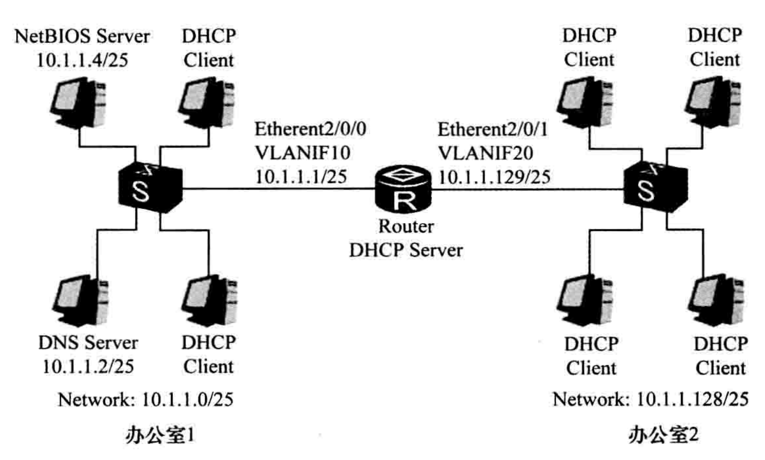


图 5-8 基于全局地址池的 DHCP 服务器配置示例基本网络结构

办公室 1 所属的网段为 10.1.1.0/25，主机都加入 VLAN10，办公室 1 的主机只使用 DNS 服务，不使用 NetBIOS 服务，地址租期为 10 天；办公室 2 所属的网段为 10.1.1.128/25，主机都加入 VLAN20，办公室 2 的主机同时使用 DNS 服务和 NetBIOS 服务，地址租期为 2 天。现要求在 Router 上配置全局地址池，采取动态地址分配方式为两个办公室的主机分配 IP 地址。

1. 基本配置思路分析

本示例是为两个 VLAN 中的 DHCP 客户端配置不同的全局地址池，所以需要在 Router 上创建两个全局地址池，并配置各自的地址池相关属性，实现根据不同需求，为办公室 1 和办公室 2 动态分配地址。然后在对应 VLANIF 接口上配置采用全局 DHCP 服务器的地址分配方式，实现 DHCP 服务器从全局地址池中给客户端分配 IP 地址的目标。

2. 具体配置步骤

根据 5.2.1 小节介绍的配置任务以及本示例的具体要求，仅需要配置 5.2.2 小节、5.2.3 小节、5.2.4 小节的配置任务（其他各小节的可选配置在本示例中没做具体要求）。

① 使能 DHCP 服务器功能。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
```

② 为 VLAN10 和 VLAN20 分别创建一个全局地址池，并按照 5.2.2 小节介绍的方法配置相关属性。在这里要特别注意的是，**路由器接口上配置的 IP 地址**（如本示例中 Ethernet2/0/0、Ethernet2/0/1 接口分别通过 VLANIF10、VLANIF20 配置的 IP 地址）**缺省已被排除在外，不用再另外排除。**

下面配置 IP 地址池 1 的属性（地址池范围、DNS 地址、出口网关、排除地址和地址池租用期）。在本地址池中仅需要排除位于 10.1.1.0/25 子网中的 DNS 服务器和 NetBIOS

服务器 IP 地址。

```
[Router] ip pool pool1
[Router-ip-pool-pool1] network 10.1.1.0 mask 255.255.255.128
[Router-ip-pool-pool1] dns-list 10.1.1.2
[Router-ip-pool-pool1] gateway-list 10.1.1.1    !---要与 VLANIF10 接口 IP 地址一致
[Router-ip-pool-pool1] excluded-ip-address 10.1.1.2
[Router-ip-pool-pool1] excluded-ip-address 10.1.1.4
[Router-ip-pool-pool1] lease day 10
[Router-ip-pool-pool1] quit
```

下面是配置 IP 地址池 2 的属性（地址池范围、DNS 地址、出口网关、NetBOIS 地址和地址池租用期）。因为 DNS 服务器和 NetBIOS 服务器 IP 地址不在本地址池所在的 10.1.1.128/25 子网内，所以也就不用配置地址排除了。

```
[Router] ip pool pool2
[Router-ip-pool-pool2] network 10.1.1.128 mask 255.255.255.128
[Router-ip-pool-pool2] dns-list 10.1.1.2
[Router-ip-pool-pool2] nbns-list 10.1.1.4
[Router-ip-pool-pool2] gateway-list 10.1.1.129
[Router-ip-pool-pool2] lease day 2
[Router-ip-pool-pool2] quit
```

③ 配置作为两个全局地址池网关的两个对应 VLANIF 接口下地址。先要把对应的物理接口加入到对应的 VLAN 中，然后为这两个 VLANIF 接口配置 IP 地址，作为两个地址池的网关。注意，为了实现两个办公室 VLAN 的互通，把这两个物理接口以不带 VLAN 标签的方式配置为 Hybrid 类型。

```
[Router] vlan batch 10 20    !---批量创建 VLAN10 和 VLAN20
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port hybrid pvid vlan 10    !---指定 Ethernet2/0/0 接口的 PVID 值为 10
[Router-Ethernet2/0/0] port hybrid untagged vlan 10
[Router-Ethernet2/0/0] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port hybrid pvid vlan 20
[Router-Ethernet2/0/1] port hybrid untagged vlan 20
[Router-Ethernet2/0/1] quit
```

④ 配置 VLANIF10 和 VLANIF20 接口 IP 地址，并使它们连接的客户端从全局地址池中获取 IP 地址。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.1 255.255.255.128
[Router-Vlanif10] dhcp select global
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.1.1.129 255.255.255.128
[Router-Vlanif20] dhcp select global
[Router-Vlanif20] quit
```

配置好后，可以通过 **display ip pool** 命令查看 IP 地址池配置情况，验证配置结果。本示例的输出如下，从中可以看出已按要求配置了两个地址池（名称分别为 pool1 和 pool2）。

```
[Router] display ip pool
 -----------------------------------------------------------------------
 Pool-name      : pool1
 Pool-No        : 0
 Position       : Local          Status          : Unlocked
```

```
Gateway-0        : 10.1.1.1
Mask             : 255.255.255.128
VPN instance     : --

-----------------------------------------------------------------
Pool-name        : pool2
Pool-No          : 1
Position         : Local             Status           : Unlocked
Gateway-0        : 10.1.1.129
Mask             : 255.255.255.128
VPN instance     : --


IP address Statistic
  Total        :250
  Used         :0          Idle        :248
  Expired      :0          Conflict    :0          Disable    :2
```

5.3 配置基于接口地址池的 DHCP 服务器

配置基于接口地址池的 DHCP 服务器，可以使从这个接口上线的用户都从该接口地址池中获取 IP 地址等分配信息。它的基本配置思想很简单，只须要配置好接口 IP 地址，然后在该接口下使能基于接口地址池 DHCP 服务器功能即可。相当于在使能了接口的基于接口地址池 DHCP 服务器功能后，系统自动创建了一个与接口的 IP 地址在同一网段的地址池，**不需要手动创建地址池**。但仍可根据需要为自动生成的接口地址池配置类似租用期、静态绑定、IP 地址排除等信息。

同样，在配置基于接口地址池的 DHCP 服务器之前，也需完成在 5.2.1 小节介绍的前期任务。完成后再根据需要完成以下配置任务（**仅第一项是必选的，其他均可根据实际需要选择配置，且与基于全局的 DHCP 地址池中的对应配置任务的配置方法一样**）。

① 配置接口地址池。

②（可选）配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务。

③（可选）配置接口地址池的 DHCP 自定义选项。

同样，因为这里涉及许多比较复杂的 DHCP Options 字段选项，且一般情况下不需配置，故在此也不作介绍。

④（可选）配置防止 IP 地址重复分配功能。

与基于全局地址池的本项配置任务的配置方法完全一样，参见 5.2.5 小节即可。

⑤（可选）配置 DHCP 数据保存功能。

与基于全局地址池的本项配置任务的配置方法完全一样，参见 5.2.6 小节即可。

⑥（可选）配置 DHCP 服务器信任 Option82 选项功能。

与基于全局地址池的本项配置任务的配置方法完全一样，参见 5.2.7 小节即可。

⑦（可选）配置 DHCP 服务器为 BOOTP 客户端分配 IP 地址。

与基于全局地址池的本项配置任务的配置方法完全一样，参见 5.2.8 小节即可。

下面仅介绍以上配置任务中的第①和第②项配置任务的具体配置方法。

5.3.1 配置接口地址池

这项配置任务主要包括使能对应接口采用接口地址池的 DHCP 服务器功能，配置接口地址池的相关属性，包括地址租期、不参与自动分配的 IP 地址以及静态绑定的 IP 地址。根据客户端的实际需要，可以选择采用动态地址分配方式或静态地址绑定方式。具体配置步骤如表 5-7 所示。

表 5-7　　接口地址池的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp enable** 例如：[Huawei] **dhcp enable**	全局使能 DHCP 服务。其他说明参见 5.2.3 小节表 5-3 中的第 2 步
3	**interface** *interface-type interface-number* 例如：**interface** gigabitethernet 1/0/0	键入要配置接口地址池的接口，进入接口视图 支持工作在接口地址池模式的接口包括三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口
4	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-GigabitEthernet1/0/0] **ip address** 10.1.1.2 24	配置以上接口的 IP 地址 命令中的参数说明参见 5.2.3 小节的表 5-3 中的第 4 步
5	**dhcp select interface** 例如：[Huawei-GigabitEthernet1/0/0] **dhcp select interface**	使能以上接口采用接口地址池的 DHCP 服务器功能 接口地址池可动态分配的 IP 地址范围就是接口的 IP 地址所在的网段，且只在此接口下有效 缺省情况下，系统未使能接口采用接口地址池的 DHCP 服务器功能，可用 **undo dhcp select interface** 命令去使能接口采用接口地址池的 DHCP 服务器功能
6	**dhcp server lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } 例如：[Huawei-GigabitEthernet1/0/0]**dhcp server lease day** 2 **hour** 2 **minute** 30	（可选）配置接口地址池中的 IP 地址租期 命令中的参数说明参见 5.2.2 小节的表 5-2 第 4 步 缺省情况下，接口地址池中 IP 地址的租用有效期限为 1 天，可用 **undo dhcp server lease** 命令恢复 IP 地址的租用有效期为缺省配置
7	**dhcp server excluded-ip-address** *start-ip-address* [*end-ip-address*] 例如：[Huawei-GigabitEthernet1/0/0]**dhcp server excluded-ip-address** 10.10.10.11 10.10.10.20	（可选）配置接口地址池中要排除分配的 IP 地址 命令中的参数说明参见 5.2.2 小节的表 5-2 第 5 步 缺省情况下，地址池中所有 IP 地址都参与自动分配，可用 **undo dhcp server excluded-ip-address** *start-ip-address* [*end-ip-address*] 命令删除指定的要被排除的 IP 地址范围
8	**dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address* 例如：[Huawei-GigabitEthernet1/0/0]**dhcp static-bind ip-address** 10.10.10.10 **mac-address** dcd2-fc96-e4c0	（可选）采用静态地址绑定方式将接口地址池中的个别 IP 地址与指定客户端的 MAC 地址进行绑定。仅当用户需要分配到固定的 IP 地址时，才需要将地址池中尚未分配的 IP 地址与用户的 MAC 地址绑定。命令中的参数说明参见 5.2.2 小节的表 5-2 第 7 步 缺省情况下，接口地址池下的 IP 地址没有与任何 MAC 地址绑定，可用 **undo dhcp server static-bind** [**ip-address** *ip-address* | **mac-address** *mac-address*]命令删除接口地址池下 IP 地址与 MAC 地址的绑定

（续表）

步骤	命令	说明
9	**dhcp server next-server** *ip-address* 例如：[Huawei-GigabitEthernet1/0/0]**dhcp next-server** 10.1.2.2	（可选）指定 DHCP 客户端启动过程中下一步使用的其他网络服务器 IP 地址。命令中的参数说明参见 5.2.2 小节的表 5-2 第 8 步 缺省情况下，DHCP 服务器未指定客户端下一步使用的其他网络服务器 IP 地址，可用 **undo dhcp server next-server** 命令恢复客户端使用的其他网络服务器 IP 地址缺省值

5.3.2 配置 DHCP 客户端的 DNS 服务和 NetBIOS 服务

为了保证 DHCP 客户端的正常通信，DHCP 服务器在给客户端分配 IP 地址的同时需指定客户端用于名称解析的 DNS 服务器或者 NetBIOS 的配置信息。用户如果不知道运营商分配的这些配置信息，可以采用动态配置的方式自动把运营商分配的 DNS 配置信息和 NetBIOS 配置信息分配给 DHCP 客户端，但静态配置方式优先。具体配置步骤如表 5-8 所示。

表 5-8 DHCP 客户端的 DNS 服务和 NetBIOS 服务的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置客户端 DNS 服务和 NetBIOS 服务的接口，进入接口视图 支持工作在接口地址池模式的接口包括：三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口
3	**dhcp server import all** 例如：[Huawei-GigabitEthernet1/0/0] **dhcp server import all**	（可选）使能接口地址池下自动获取 DNS 和 NetBIOS 服务器的配置信息，**可以单独配置，也可以与下面介绍的静态配置同时配置，但同时配置时，静态配置优先** 缺省情况下，接口地址池下动态获取 DNS 和 NetBIOS 服务器配置信息的功能处于未使能状态，可用 **undo dhcp server import all** 命令去使能接口地址池下动态获取 DNS 和 NetBIOS 服务器的配置信息 其他说明参见 5.2.4 小节表 5-4 中的第 3 步
4	**dhcp server domain-name** *domain-name* 例如：[Huawei-GigabitEthernet1/0/0] **domain-name** huawei.com	（可选）配置为 DHCP 客户端静态分配的域名后缀。缺省情况下，系统未配置为 DHCP 客户端分配的域名后缀，可用 **undo dhcp server domain-name** 命令删除为对应接口地址池中的 DHCP 客户端配置的域名后缀 其他说明参见 5.2.4 小节表 5-4 中的第 4 步
5	**dhcp server dns-list** *ip-address* &<1-8> 例如：[Huawei-GigabitEthernet1/0/0]**dns-list** 10.10.10.10	（可选）配置 DHCP 客户端使用的 DNS 服务器的 IP 地址。缺省情况下，接口地址池下未配置 DNS 服务器地址，可用 **undo dhcp server dns-list** { *ip-address* | **all** }命令删除对应接口地址池下指定的或者全部 DNS 服务器 IP 地址 其他说明参见 5.2.4 小节表 5-4 中的第 5 步
6	**dhcp server nbns-list** *ip-address* &<1-8> 例如：[Huawei-GigabitEthernet1/0/0] **nbns-list** 1.1.1.1	（可选）配置 DHCP 客户端的 NetBIOS 服务器地址。缺省情况下，接口地址池中没有配置 NetBIOS 服务器，可用 **undo dhcp server nbns-list** { *ip-address* | **all** }命令删除对应接口地址池下指定的或者全部 NetBIOS 服务器 IP 地址 其他说明参见 5.2.4 小节表 5-4 中的第 6 步

（续表）

步骤	命令	说明
7	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } 例如：[Huawei-GigabitEthernet1/0/0] **netbios-type b-node**	（可选）配置 DHCP 客户端的 NetBIOS 节点类型。缺省情况下，不指定客户端的 NetBIOS 节点类型，可用 **undo dhcp server netbios-type** 命令恢复缺省配置 其他说明参见 5.2.4 小节表 5-4 中的第 7 步

5.3.3 基于接口地址池的 DHCP 服务器的配置示例

本示例的基本网络结构如图 5-9 所示。某企业有两个处于同一网络内的办公室，为了节省资源，两个办公室内的主机由 Router 作为 DHCP 服务器统一为内网用户分配 IP 地址。办公室 1 所属的网段为 10.1.1.0/24，主机都加入 VLAN10，办公室 1 使用 DNS 服务和 NetBIOS 服务，地址租期 3 天；办公室 2 所属的网段为 10.1.2.0/24，主机都加入 VLAN20，办公室 2 不使用 DNS 服务和 NetBIOS 服务，地址租期 2 天。现要配置基于接口地址池的 DHCP 服务器，解决在同一网络内的客户端从服务器获取 IP 地址问题。

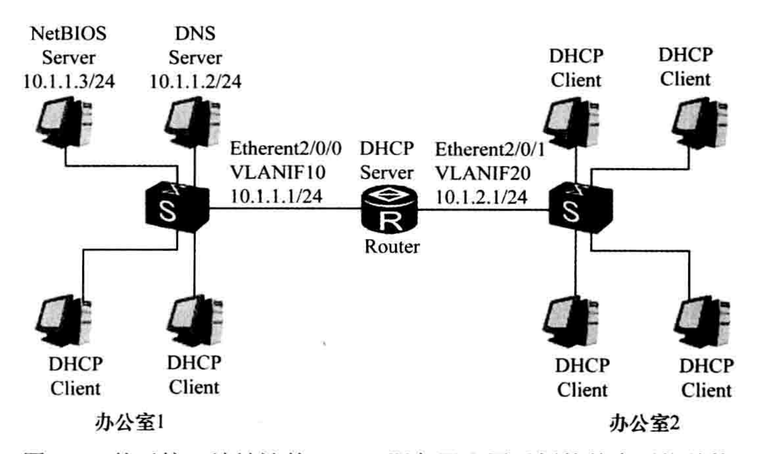


图 5-9　基于接口地址池的 DHCP 服务器配置示例的基本网络结构

1. 基本配置思路分析

本示例是要为两个 VLAN 中的 DHCP 客户端配置不同的接口地址池，可以在 Router 上两个对应接口下创建两个接口地址池（**其实并不需要手动创建这两个地址池，只须在对应 VLANIF 接口使能基于接口的 DHCP 服务器功能即可**），并配置各自的地址池相关属性，实现 DHCP 服务器从基于接口的地址池中选择 IP 地址分配给办公室主机的目的。

2. 具体配置步骤

根据 5.3 节介绍的配置任务以及本示例的具体要求，仅需要配置 5.3.1 小节和 5.3.2 小节的配置任务（其他可选配置在本示例中没做具体要求）。

① 在 Router 上使能 DHCP 服务。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
```

② 在 Router 上创建两个 VLAN，然后分别把 Ethernet2/0/0 和 Ethernet2/0/1 LAN 接

口加入 VLAN10、VLAN20 中。如果两个 VLAN 是通过一个物理接口与 Router 连接的话，则需要配置两个子接口封装对应的 VLAN（也就是通常所说的“单臂路由”）。

```
[Router] vlan batch 10 20
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port hybrid pvid vlan 10
[Router-Ethernet2/0/0] port hybrid untagged vlan 10
[Router-Ethernet2/0/0] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port hybrid pvid vlan 20
[Router-Ethernet2/0/1] port hybrid untagged vlan 20
[Router-Ethernet2/0/1] quit
```

再配置两个 VLANIF 接口的 IP 地址，并使能接口连接的客户端从接口地址池中获取 IP 地址。如果是通过子接口封装两个 VLAN 时，则需要在子接口上进行配置。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.1 255.255.255.0
[Router-Vlanif10] dhcp select interface
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.1.2.1 255.255.255.0
[Router-Vlanif20] dhcp select interface
[Router-Vlanif20] quit
```

③ 配置 VLANIF10 接口对应地址池的 DNS 服务器、NetBOIS 服务器、排除 IP 地址。因为在本示例中，办公室 2 不需要用到 DNS 和 NetBIOS 服务进行名称解析，所以不需要在 VLNIF20 下进行类似配置。

```
[Router] interface vlanif 10
[Router-Vlanif10] dhcp server domain-name huawei.com
[Router-Vlanif10] dhcp server dns-list 10.1.1.2
[Router-Vlanif10] dhcp server nbns-list 10.1.1.3
[Router-Vlanif10] dhcp server excluded-ip-address 10.1.1.2
[Router-Vlanif10] dhcp server excluded-ip-address 10.1.1.3
```

④ 配置两个 VLANIF 接口地址池中地址租用期限。

```
[Router] interface vlanif 10
[Router-Vlanif10] dhcp server lease day 3
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] dhcp server lease day 2
[Router-Vlanif20] quit
```

接口地址池配置好后，可以通过 **display ip pool interface** 命令分别查看两 VLANIF 接口下的地址池配置情况，验证配置结果。下面是本示例中 VLANIF10 接口下的输出。

```
[Router] display ip pool interface vlanif10
 Pool-name        : vlanif10
 Pool-No          : 0
 Lease            : 3 Days 0 Hours 0 Minutes
 Domain-name       : huawei.com
 DNS-Server0       : 10.1.1.2
 NBNS-Server0      : 10.1.1.3
 Netbios-type     : b-node
 Position         : Interface        Status            : Unlocked
 Gateway-0         : 10.1.1.1
```

```
Mask             : 255.255.255.0
VPN instance     : --
---------------------------------------------------------------------------------
     Start          End      Total  Used  Idle(Expired)  Conflict  Disable
---------------------------------------------------------------------------------
   10.1.1.1    10.1.1.254   253     0    251(0)             0         2
---------------------------------------------------------------------------------
```

5.4 配置 DHCP 中继

当 DHCP 客户端与 DHCP 服务器之间经过三层设备相连时（此时 DHCP 客户端与 DHCP 服务器不在同一网段中），DHCP 客户端就不能直接与 DHCP 服务器进行 DHCP 通信。这时就需要通过 DHCP 中继设备在中间担当一个中间代理角色，负责转发 DHCP 客户端与 DHCP 服务器之间的 DHCP 通信。同时，这样多个网段的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于集中管理。

【经验之谈】 DHCP 中继是直接与 DHCP 所在网段客户端连接的，**但不一定要与 DHCP 服务器所在网段直接连接**，所以在配置 DHCP 中继之前，除了需要先配置好 DHCP 服务器外，还要确保 DHCP 中继到达 DHCP 服务器的路由畅通。

AR G3 系列路由器作为 DHCP 中继时所包括的主要配置任务如下。

① 配置指定接口工作在 DHCP 中继模式。

②（可选）配置 DHCP 中继转发的目的 DHCP 服务器组（**仅当 DHCP 中继设备需要为多个 DHCP 服务器进行报文转发时才需要配置**）。

③ 配置 DHCP 中继接口绑定 DHCP 服务器或 DHCP 服务器组。

④（可选）配置 DHCP 中继请求 DHCP 服务器释放客户端 IP 地址（**仅当 DHCP 客户端需要请求释放 IP 地址时才需要执行**）。

下面各小节将分别介绍以上配置任务的具体配置步骤。

5.4.1 配置指定接口工作在 DHCP 中继模式

DHCP 中继模式仅可在三层模式的接口（**是指 DHCP 中继连接 DHCP 客户端的接口**）上配置，并且首先需要全局使能 DHCP 服务功能（将同时使能所有 DHCP 服务功能，包括 DHCP 服务器、DHCP 客户端、DHCP 中继和 DHCP Snooping），然后在该接口上使能 DHCP 中继功能。当然，还可配置一些其他可选功能，如 DHCP 服务器的轮询功能和对 Options 选项的支持。具体配置步骤如表 5-9 所示。

表 5-9　在指定接口上使能 DHCP 中继功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**dhcp enable** 例如：[Huawei] **dhcp enable**	使能路由器的 DHCP 服务功能，在使能了 DHCP 服务功能的同时将使能 DHCP 中继功能 其他说明参见 5.2.3 小节表 5-3 中的第 2 步

（续表）

步骤	命令	说明
3	**ip relay address cycle** 例如：[Huawei] **ip relay address cycle**	（可选）配置 DHCP 中继的轮询功能，仅当 DHCP 中继设备需要向多个 DHCP 服务器转发 DHCP 报文时才需要配置。因为当 DHCP 中继上配置多个 DHCP 服务器时，DHCP 中继会默认向所有的服务器转发 DHCP DISCOVER 报文，这样会造成 DHCP 中继的负担较重。执行此命令后，DHCP 客户端发送 DHCP DISCOVER 报文时，DHCP 中继只会选择其中一个 DHCP 服务器进行轮询转发，如果没有收到这个 DHCP 服务器的响应，则继续向另外一个 DHCP 服务器转发 DHCP DISCOVER 报文，依此类推，直到接收到响应报文 缺省情况下，DHCP 中继的轮询功能处于未使能状态，可用 **undo ip relay address cycle** 命令去使能 DHCP 中继的轮询功能
4	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入连接 DHCP 客户端的 DHCP 中继设备三层接口，进入接口视图 支持工作在 DHCP 中继模式的接口可以是三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VLANIF 接口
5	**ip address** *ip-address* { *mask* | *mask-length* } 例如：[Huawei-GigabitEthernet1/0/0] **ip address** 129.102.0.1 255.255.255.0	为以上 DHCP 中继接口配置 IP 地址 **该接口 IP 地址必须与 DHCP 服务器上配置的客户端的出口网关地址保持一致**
6	**dhcp select relay** 例如：[Huawei-GigabitEthernet1/0/0]**dhcp select relay**	在以上三层接口上使能 DHCP 中继功能 **【注意】DHCP 服务器与 DHCP 中继相连的接口上不允许再配置接口地址池** 如果指定子接口工作在 DHCP 中继模式，则需要在子接口上配置 **arp broadcast enable** 命令，使能终结子接口的 ARP 广播功能 如果在一个 Super-Vlan 接口上使能了 DHCP 中继功能，则该 Super-Vlan 接口不能再使能 DHCP Snooping 功能 缺省情况下，系统未使能 DHCP 中继功能，可用 **undo dhcp select relay** 命令去使能接口的 DHCP 中继功能
7	**quit** 例如：[Huawei-GigabitEthernet1/0/0] **quit**	退出接口视图，返回系统视图
8	**dhcp relay trust option82** 例如：[Huawei] **dhcp relay trust option82**	（可选）使能 DHCP Relay 信任 Option82 选项功能，使在 DHCP 中继在收到 DHCP 请求报文时，如果其中包含了 Option82 信息，但当 giaddr 字段为 0 时，缺省情况下设备将继续对报文进行处理，但如果配置了 **undo dhcp relay trust option82** 命令，设备将不对该报文进行处理 缺省情况下，系统使能信任 option82 选项功能，可用 **undo dhcp relay trust option82** 命令去使能 DHCP Relay 信任 Option82 选项功能，丢弃包含了 Option82 信息，但 giaddr 字段为 0 的 DHCP 请求报文

5.4.2 配置 DHCP 中继转发的目的 DHCP 服务器组

因为当路由器担当 DHCP 中继角色时可以向多个 DHCP 服务器进行报文转发，故可在 DHCP 中继设备上配置一个包括多个 DHCP 服务器的服务器组。当然，DHCP 服务器组中也可仅包括一个 DHCP 服务器。但采用这种配置方式时通常是**仅需要在 DHCP 中继接口上绑定多个 DHCP 服务器时可选进行**。具体配置步骤如表 5-10 所示。

表 5-10 DHCP 服务器组的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp server group** *group-name* 例如：[Huawei] **dhcp server group** dhcp-srv1	创建 DHCP 服务器组，进入 DHCP 服务器组视图。参数 *group-name* 用来指定所创建的 DHCP 服务器组的名称，为 1～32 个字符，区分大小写，不支持空格 全局最多可以配置 64 个 DHCP 服务器组 缺省情况下，系统未配置 DHCP 服务器组，可用 **undo dhcp server group** *group-name* 命令删除已经创建的指定 DHCP 服务器组
3	**dhcp-server** *ip-address* [*ip-address-index*] 例如：[Huawei-dhcp-server-group-dhcp-srv1] **dhcp-server** 10.10.78.56	向以上 DHCP 服务器组中添加一个 DHCP 服务器 IP 地址。命令中的参数说明如下。 ● *ip-address*：指定要添加的 DHCP 服务器 IP 地址 ● *ip-address-index*：可选参数，指定 DHCP 服务器 IP 地址索引号，取值范围为 0～7 的整数。**如果不指定索引，此时系统将自动分配一个空闲的索引号** 每个 DHCP 服务器组下最多可以配置 8 个 DHCP 服务器，如要添加多个 DHCP 服务器地址时，则需要多次执行本命令 缺省情况下，DHCP 服务器组下未配置 DHCP 服务器成员，可用 **undo dhcp-server** { *ip-address* | *ip-address-index* } 命令从 DHCP 服务器组中删除指定的 DHCP 服务器成员
4	**gateway** *ip-address* 例如：[Huawei-dhcp-server-group-dhcp-srv1]**gateway** 10.10.10.1	（可选）配置 DHCP 中继到达 DHCP 服务器的网关地址，**仅当 DHCP 服务器和 DHCP 中继不在同一网段时才需要配置**。在另一方，DHCP 服务器也需要使用 **gateway-list** *ip-address* &<1-8>命令建立到达 DHCP 中继的网关地址 【注意】在 DHCP 中继上如果不用 **gateway** 命令建立出口网关，则默认使用 DHCP 中继上的接口地址与 DHCP 服务器建立通信，所以**一般不用配置**。在 DHCP 服务器和 DHCP 中继都使用 AR G3 系列设备的情况下，**这里配置的网关地址和 DHCP 服务器上配置的网关地址必须完全一致** 缺省情况下，系统未配置网关地址，可用 **undo gateway** 命令恢复缺省配置
5	**vpn-instance** *vpn-instance-name* 例如：[Huawei-dhcp-server-group-dhcp-srv1]**vpn-instance vpn-1**	（可选）将 DHCP 服务器组绑定到已创建好的 VPN 实例。参数 *vpn-instance-name* 用来指定 VPN 实例名称，1～31 个字符，区分大小写，不支持空格，可以设定为包含数字、字母和下划线“_”或“.”的组合 【注意】DHCP 中继的服务器组绑定的 VPN 实例必须与 DHCP 服务器端地址池绑定的 VPN 实例一致，接口下的用户才可以通过该 DHCP 服务器组上线 缺省情况下，DHCP 服务器组未绑定 VPN 实例，可用 **undo vpn-instance** 命令删除 DHCP 服务器组绑定的 VPN 实例

5.4.3 配置 DHCP 中继接口绑定 DHCP 服务器或 DHCP 服务器组

使能了 DHCP 中继设备连接 DHCP 服务器的接口的中继功能后，就可以在 DHCP 中继接口上绑定上节创建的 DHCP 服务器组，从而为 DHCP 客户端指定可以访问的 DHCP 服务器。

当然，如果 DHCP 中继接口仅需要与一个 DHCP 服务器进行绑定，也可以不用绑定 DHCP 服务器组，而是直接配置所要代理的 DHCP 服务器。具体的配置步骤如表 5-11 所示。

表 5-11　　中继接口绑定 DHCP 服务器或 DHCP 服务器组的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number*	键入 DHCP 中继接口，进入接口视图
3	**dhcp relay server-select** *group-name* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp relay server-select** dhcp-srv1	（二选一）指定接口要绑定的 DHCP 服务器组。参数 *group-name* 用来指定上节表 5-10 第 2 步所创建的，需要在中继接口上绑定的 DHCP 服务器组名称 缺省情况下，接口未指定 DHCP 服务器组，可用 **undo dhcp relay server-select** 命令删除 DHCP 中继所对应的 DHCP 服务器组
	dhcp relay server-ip *ip-address* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp relay server-ip** 1.1.1.3	（二选一）配置 DHCP 中继所绑定的单个 DHCP 服务器地址。如果需要绑定多个 DHCP 服务器地址，可重复执行该命令 缺省情况下，接口下没有配置 DHCP 服务器地址，可用 **undo dhcp relay server-ip** { *ip-address* | **all** }命令删除配置的指定或者所有 DHCP 服务器地址

5.4.4 配置 DHCP 中继请求 DHCP 服务器释放客户端 IP 地址

在某些情况下，比如强制某用户下线等，可以手动释放 DHCP 服务器上给用户分配的 IP 地址。配置 DHCP 中继请求 DHCP 服务器释放客户端的 IP 地址功能后，DHCP 中继会主动向指定的 DHCP 服务器发送 Release 报文，DHCP 服务器收到该报文后，将会释放指定 IP 地址的租约。

可在系统视图下或者 DHCP 中继接口视图下请求 DHCP 服务器释放客户端 IP 地址，具体配置方法很简单，仅须执行 **dhcp relay release** *client-ip-address mac-address* [**vpn-instance** *vpn-instance-name*] [*server-ip-address*]命令即可。命令中的参数说明如下。

① *client-ip-address*：指定要释放的 DHCP 客户端 IP 地址。

② *mac-address*：指定要释放 IP 地址的 DHCP 客户端 MAC 地址。

③ **vpn-instance** *vpn-instance-name*：可选参数，指定要释放 IP 地址的 DHCP 客户端所在的 VLN 实例名称，**但在接口视图下不支持**。

④ *server-ip-address*：可选参数，指定要释放 IP 地址的 DHCP 服务器 IP 地址。

在系统视图下执行时：如果不指定 DHCP 服务器（即 *server-ip-address* 参数），则向所有配置为中继模式的接口所绑定的所有 DHCP 服务器发送释放申请；如果指定了

DHCP 服务器的 IP 地址，则只向指定 DHCP 服务器发送释放申请；在接口视图下执行时：如果不指定 DHCP 服务器，则向该接口所绑定的所有 DHCP 服务器发送释放申请；如果指定了 DHCP 服务器的 IP 地址，则只向指定 DHCP 服务器发送释放申请。

5.4.5　不同网段内 DHCP 服务器和 DHCP 中继的配置示例

本示例的基本网络结构如图 5-10 所示，某公司拥有多个办公地点且位于不同的商务楼宇中，不同楼宇内的办公室主机在不同的 VLAN 内，公司希望不同办公地点、不同网段的主机由共同的 DHCP 服务器 RouterB 分配 IP 地址。其中，公司的办公地点 A 的主机所在的网段为 20.20.20.0/24，而 DHCP 服务器所在的网段为 100.10.10.0/24。通过带 DHCP 中继功能的 RouterA 转发 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。RouterA 上接口 GE1/0/0 的公网地址为 100.10.20.1/24，对端运营商侧地址为 100.10.20.2/24；RouterB 上接口 GE1/0/0 的公网地址为 100.10.10.1/24，对端运营商侧地址为 100.10.10.2/24。

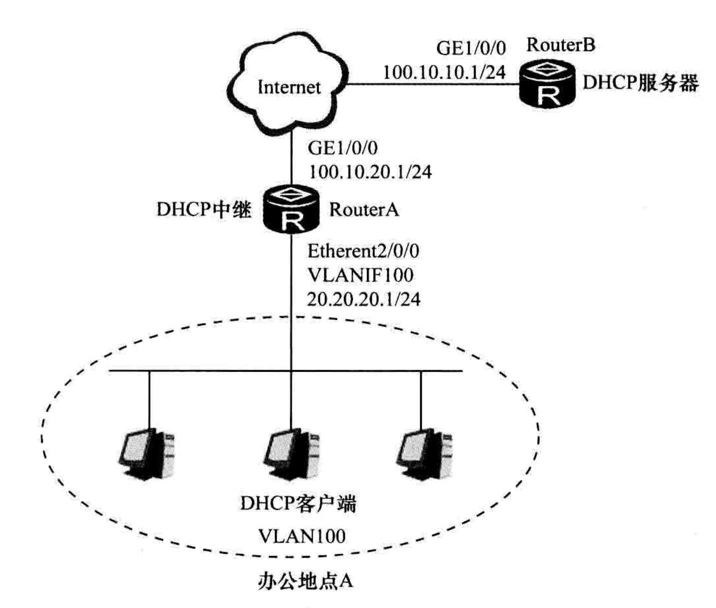


图 5-10　DHCP 中继配置示例的基本网络结构

1. 基本配置思路分析

本示例同时涉及 DHCP 中继和 DHCP 服务器配置。基本配置思路如下。

① 在 RouterA 上 VLANIF100 接口上使能 DHCP 中继功能，实现 RouterA 转发不同网段的 DHCP 报文功能。因为缺省使用的就是 DHCP 中继接口为出口网关，故可不用配置到达 DHCP 服务器的出口网关。

② 在 RouterB 上配置一个 IP 地址范围为 20.20.20.0/24 的全局地址池，实现 DHCP 服务器为位于不同网段的 DHCP 客户端分配 IP 地址。DHCP 服务器上全局地址池的配置仅配置必须要配置的配置任务，可选配置任务可不作配置，参见 5.2.1 小节。

2. 具体配置步骤

（1）RouterA 上 DHCP 中继功能配置

① 在接口下使能 DHCP 中继功能。先要把 RouterA 上的 Ethernet2/0/0 加入到 VLAN100 中（因为 Ethernet2/0/0 接口是与 Internet 连接的，不能识别 VLAN，所以要配置为不带标签的 Hybrid 接口类型），然后配置 VLANIF100 接口的 IP 地址，使能 VLANIF100 接口上的 DHCP 中继功能。

```
[RouterA] vlan batch 100
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port hybrid pvid vlan 100
[RouterA-Ethernet2/0/0] port hybrid untagged vlan 100
[RouterA-Ethernet2/0/0] quit
[RouterA] dhcp enable   !---全局使能 DHCP 服务功能
[RouterA] interface vlanif 100
[RouterA-Vlanif100] ip address 20.20.20.1 24
[RouterA-Vlanif100] dhcp select relay   !---在 VLANIF100 接口上使能 DHCP 中继功能
[RouterA-Vlanif100] quit
```

② 创建 DHCP 服务器组并为服务器组添加 DHCP 服务器。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dhcp server group dhcpgroup1
[RouterA-dhcp-server-group-dhcpgroup1] dhcp-server 100.10.10.1
[RouterA-dhcp-server-group-dhcpgroup1] quit
```

说明 因为本示例中仅有一台 DHCP 服务器，所以也可以不创建 DHCP 服务器组，而是直接在 DHCP 中继接口视图下使用 **dhcp relay server-ip** 100.10.10.1 接口视图命令指定所代理的 DHCP 服务器。

③ 配置 VLANIF100 接口绑定前面创建的 DHCP 服务器组。

```
[RouterA] interface vlanif 100
[RouterA-Vlanif100] dhcp relay server-select dhcpgroup1
[RouterA-Vlanif100] quit
```

④ 在 RouterA 上配置到达 DHCP 服务器 RouterB 的缺省路由（以 RouterA 对端运营商 IP 地址为下一跳）。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 100.10.20.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] ip route-static 0.0.0.0 0.0.0.0 100.10.20.2
```

（2）RouterB 上全局地址池配置

① 使能 DHCP 服务。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] dhcp enable
```

② 配置 GE1/0/0 接口 IP 地址，并使其工作在全局地址池模式。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 100.10.10.1 24   !---这个 IP 地址不能与地址池的 IP 地址在同一网段
[RouterB-GigabitEthernet1/0/0] dhcp select global
[RouterB-GigabitEthernet1/0/0] quit
```

③ 创建地址池并配置出口网关列表。

```
[RouterB] ip pool pool1
[RouterB-ip-pool-pool1] network 20.20.20.0 mask 24
[RouterB-ip-pool-pool1] gateway-list 20.20.20.1   !---配置分配地址时的出口网关地址为 VLANIF100 接口 IP 地址
[RouterB-ip-pool-pool1] quit
```

④ 在 RouterB 上配置到达 DHCP 中继 RouterA 的缺省路由（以 RouterB 对端运营商 IP 地址为下一跳）。

```
[RouterB] ip route-static 0.0.0.0 0.0.0.0 100.10.10.2
```

配置好后，可在 RouterA 上使用 **display dhcp relay interface** vlanif 100 命令查看接口的 DHCP 中继配置情况。在 RouterB 上可使用 **display ip pool** 命令用来查看 IP 地址池配置情况。具体如下。

```
[RouterA] display dhcp relay interface vlanif 100
 DHCP relay agent running information of interface Vlanif100 :
 Server group name : dhcpgroup1
 Gateway address in use : 20.20.20.1

[RouterB] display ip pool
   -----------------------------------------------------------------------
  Pool-name        : pool1
  Pool-No          : 0
  Position         : Local          Status          : Unlocked
  Gateway-0        : 20.20.20.1
  Mask             : 255.255.255.0
  VPN instance     : --


 IP address Statistic
    Total       :253
    Used        :1          Idle        :253
    Expired     :0          Conflict    :0          Disable    :0
```

5.5 配置 DHCP/BOOTP 客户端

AR G3 系列路由器也可配置作为 DHCP 或者 BOOTP 客户端使用，通过 DHCP 协议使其接口可从指定的 DHCP 服务器动态获得 IP 地址及其他配置信息。

在配置 DHCP/BOOTP 客户端之前，需完成以下任务。

① 配置 DHCP 服务器。

② 配置 DHCP 中继（据实际需要，可选择配置）。

③ 配置路由器到 DHCP 中继或 DHCP 服务器的路由。

把 AR G3 系列路由器配置成 DHCP 或者 BOOTP 客户端的主要配置任务如下（**仅最后一项是必选的**，其他属性均有缺省值，可根据实际需要修改配置）。

①（可选）配置 DHCP/BOOTP 客户端属性。

②（可选）配置 DHCP 服务器路由下发属性。

③ 使能 DHCP/BOOTP 客户端功能。

5.5.1 配置 DHCP/BOOTP 客户端属性

DHCP/BOOTP 客户端属性配置主要包括配置 DHCP 客户端的主机名、标识、Option60 字段、网关探测功能、期望租期，并使能 DHCP 服务。通过配置 DHCP/BOOTP 客户端属性，有助于 DHCP/BOOTP 客户端和 DHCP 服务器之间的通信。具体配置步骤

如表 5-12 所示（**属性之间没有严格的配置次序**），要注意的是，其中多数配置仅适用于 DHCP 客户端，已用粗体字特别强调。

表 5-12 DHCP/BOOTP 客户端属性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp enable** 例如：[Huawei] **dhcp enable**	使能 DHCP 服务。参见 5.2.3 小节表 5-3 中的第 2 步
3	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要使能 DHCP 或者 BOOTP 客户端功能的接口（连接客户端侧的三层接口），进入接口视图 支持工作在 DHCP 客户端的接口可以是三层 GE 接口及其子接口、三层 Ethernet 接口及其子接口、三层 Eth-trunk 接口及其子接口和 VE 接口
4	**dhcp client class-id** *class-id* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client class-id** huawei	配置 **DHCP 客户端**发送 DHCP 请求报文中的 Option60 字段（用来设置厂商分类信息选项，标识 DHCP 客户端的类型和配置），1～64 个字符，区分大小写 【说明】DHCP 服务器需要根据请求报文中的 Option60 字段内容来区分不同设备，用户可以使用此命令自定义设备作为 DHCP 客户端时，发送的请求报文中封装的 Option60 内容接口下。配置此命令后，设备作为 DHCP 客户端时（包括 auto-config 时获取地址阶段），从该接口发送的 DHCP 请求报文中将使用配置的内容填充 Option60 字段 缺省情况下，未配置 Option60 字段，可用 **undo dhcp client class-id** 命令删除已配置的 DHCP 请求报文中的 Option60 字段
5	**dhcp client hostname** *hostname* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client hostname** huawei gateway	配置 **DHCP 客户端或 BOOTP 客户端**的主机名，1～64 个字符，**支持空格，但区分大小写** 缺省情况下，系统未配置 DHCP/BOOTP 客户端的主机名，可用 **undo dhcp client hostname** 命令删除配置的 DHCP/BOOTP 客户端的主机名
6	**dhcp client client-id** *client-id* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client client-id** huawei_client	配置 **DHCP 客户端**的标识，1～64 个字符，**不支持空格，区分大小写** 【说明】DHCP 客户端在申请 IP 地址的时候，DHCP 服务器会获取请求报文中的 DHCP 客户端标识信息，DHCP 服务器将根据该标识，为 DHCP 客户端分配 IP 地址 缺省情况下，DHCP 客户端的标识是客户端的 MAC 地址，可用 **undo dhcp client client-id** 命令恢复 DHCP 客户端的标识为缺省值
7	**dhcp client gateway-detect period** *period* **retransmit** *retransmit* timeout *time* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client gateway-detect period** 3600 **retransmit** 3 **timeout** 500	配置 **DHCP 客户端**的网关探测功能。命令中的参数说明如下 • **period** *period*：指定 DHCP 客户端的网关探测周期，取值范围为 1～86 400 的整数秒 • **retransmit** *retransmit*：指定 DHCP 客户端的网关探测的重传次数，取值范围为 1～10 的整数 • **timeout** *time*：指定 DHCP 客户端的网关探测的超时时间，取值范围为 1～1 000 的整数秒

（续表）

步骤	命令	说明
7	**dhcp client gateway-detect period** *period* **retransmit** *retransmit* timeout *time* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client gateway-detect period** 3600 **retransmit** 3 **timeout** 500	【注意】DHCP 客户端网关探测功能**仅适用于双上行链路场景**，这时，当 DHCP Client 成功获取 IP 地址后，该功能可以使 DHCP Client 迅速检测正在使用的网关状态，如果当前网关地址错误或网关设备故障，DHCP 客户端就可以通过其他上行链路（即其他网关）将向 DHCP 服务器重新发送 IP 地址请求 缺省情况下，系统未配置 DHCP 客户端网关探测功能，可用 **undo dhcp client gateway-detect** 命令删除配置的 DHCP 客户端网关探测功能
8	**dhcp client expected-lease** *time* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client expected-lease** 7200	配置 **DHCP 客户端**期望的租期时间。参数 *time* 用来指定 DHCP 客户端期望租期时间，取值范围为 60～864 000 的整数秒 【说明】DHCP 客户端向服务器申请地址时，可以携带期望地址租用期，该信息存放于报文的 Option51 字段中。当服务器在分配地址租约时，会把客户端期望租用时间和地址池中的地址租用期进行比较，选择其中一个时间较短的租期分配给 DHCP 客户端 缺省情况下，系统未配置 DHCP 客户端期望的租用时间，可用 **undo dhcp client expected-lease** 命令删除 DHCP 客户端期望的租用时间

5.5.2　配置 DHCP 服务器路由下发属性

当 DHCP 客户端发送 DHCP 请求后，DHCP 服务器可以分配给客户端 IP 地址以及其他网络配置参数。DHCP 服务器还可以下发路由表项给 DHCP 客户端，动态刷新客户端路由表。还可以配置 DHCP 客户端通过 DHCP 方式获取的路由表及路由表项优先级，具体配置步骤如表 5-13 所示。

表 5-13　　DHCP 服务器路由下发属性的配置步骤

1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ip route** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*] 例如：[Huawei] **ip route** 1.1.1.1 24 gigabitethernet 0/0/1 **dhcp** 30	配置 DHCP 客户端通过 DHCP 方式获取的路由表，实现动态刷新客户端路由表。命令中的参数说明如下 ● *ip-address*：指定路由表中的目的 IP 地址 ● { *mask* | *mask-length* }：指定以上 IP 地址对应的子网掩码（选择 *mask* 参数时）或子网掩码长度（选择 *mask-length* 参数时） ● *interface-number*：指定转发路由报文到 DHCP 客户端的接口类型和接口号 ● **dhcp**：指定通过 DHCP 方式获取路由表 ● *preference-value*：可选参数，指定路由的优先级，取值范围为 1～255 的整数 缺省情况下，系统未配置 DHCP 客户端通过 DHCP 方式获取的路由表，可用 **undo ip route** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]命令删除配置的 DHCP 方式获取的路由表

（续表）

3	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入 DHCP 客户端接口（也就是希望从 DHCP 服务器自动分配 IP 地址的接口），进入接口视图
4	**dhcp client default-route preference** *preference-value* 例如：[Huawei-GigabitEthernet1/0/0] **dhcp client default-route preference** 30	配置 DHCP 服务器下发给以上接口下连接的 DHCP 客户端的路由表项的默认优先级，取值范围为 1～255 的整数 缺省情况下，DHCP 服务器下发给 DHCP 客户端的路由表项默认优先级为 60，可用 **undo dhcp client default-route preference** 命令恢复DHCP服务器下发给DHCP客户端的路由表项默认优先级为缺省值

5.5.3 使能 DHCP/BOOTP 客户端功能

在 DHCP/BOOTP 客户端配置任务中，DHCP/BOOTP 客户端功能的使能必须放在最后进行，否则路由器会使用错误的属性配置来从 DHCP 服务器获取 IP 地址。

使能 DHCP/BOOTP 客户端功能的方法很简单，就是在对应的 DHCP 或者 BOOTP 客户端接口视图下分别执行 **ip address dhcp-alloc** 或者 **ip address bootp-alloc** 命令。缺省情况下，接口下 DHCP、BOOTP 客户端功能处于未使能状态，分别可用 **undo ip address dhcp-alloc** 或 **undo ip address bootp-alloc** 命令去使能接口下的DHCP或BOOTP客户端功能。

5.6 配置 DHCP 报文限速

为了避免受到攻击者发送大量 DHCP 报文的攻击，可以在设备上配置 DHCP 报文限速功能，以检查 DHCP 报文，并限制报文的上送速率，这样在一定的时间内只允许规定数目的报文上送协议栈，多余的报文将被丢弃。

5.6.1 DHCP 报文限速配置步骤

DHCP 报文限速可以在系统视图下配置，也可以在 VLAN 视图下配置，或者在 DHCP 服务接口（使能了 DHCP 服务器，或者 DHCP 中继功能的接口）视图下配置。**用户可以根据实际需要选择其中一种配置方式，也可以同时在全局模式、VLAN 或接口下进行配置，同时配置生效优先级从高到低的顺序是接口最高，VLAN 其次，全局模式最低。**

本项配置任务也是可选的，因为其中的参数都有对应的缺省配置，可根据实际需要选择修改。以上三种情形下的 DHCP 报文限速具体配置步骤如表 5-14 所示。但在配置此项任务之前先要配置好 DHCP 服务器或者 DHCP 中继。

表 5-14 DHCP 报文限制配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp enable** 例如：[Huawei] **dhcp enable**	使能 DHCP 功能 其他说明参见 5.2.3 小节表 5-3 中的第 2 步

（续表）

步骤	命令	说明
方式 1：在系统视图下配置 DHCP 报文限速		
3	**dhcp check dhcp-rate enable** [**vlan** { *vlan-id1* [to *vlan-id2*] } &<1-10>] 例如：[Huawei] **dhcp check dhcp-rate enable vlan** 2 **to** 10	使能 DHCP 报文速率检查功能。命令中的参数说明如下 ● **vlan** { *vlan-id1* [**to** *vlan-id2*] }：可选参数，指定使能 DHCP 报文速率检查功能的 VLAN 范围。如果不指定本参数，则 DHCP 服文限速功能将在网络中所有 VLAN 中使能 ● &<1-10>：可选参数，指定前面的{ *vlan-id1* [**to** *vlan-id2*] 参数最多可以有 10 个，之间用空格分隔 缺省情况下，不使能 DHCP 报文速率检查功能，可用 **undo dhcp check dhcp-rate enable** [vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]命令去使能指定 VLAN 或者全部 VLAN 中的 DHCP 报文速率检查功能
4	**dhcp check dhcp-rate** *rate* [**vlan** { *vlan-id1* [to *vlan-id2*] } &<1-10>] 例如：[Huawei] **dhcp check dhcp-rate** 50 **vlan** 2 **to** 10	配置 DHCP 报文上送到 DHCP 协议栈的检查速率。命令中的参数说明如下 ● *rate*：指定上送到 DHCP 协议栈的检查速率，取值范围为（1～100）整数个 pps ● **vlan** { *vlan-id1* [**to** *vlan-id2*] }：可选参数，指定以上 *rate* 参数的检查速率配置所作用的 VLAN 范围。如果不指定本参数，则以上检查速率配置将作用于网络中所有 VLAN 中 ● &<1-10>：可选参数，指定前面的{ *vlan-id1* [**to** *vlan-id2*] 参数最多可以有 10 个，之间用空格分隔 缺省情况下，上送的 DHCP 报文速率限制在 100 pps 以内（超过此速率限制的 DHCP 报文会被丢弃），可用 **undo dhcp check dhcp-rate** 命令恢复 DHCP 报文上送到 DHCP 协议栈的检查速率为缺省值
方式 2：在 VLAN 视图下配置 DHCP 报文限速		
3	**vlan** *vlan-id* 例如：[Huawei] **vlan** 10	键入要配置 DHCP 报文限速的 VLAN，进入 VLAN 视图
4	**dhcp check dhcp-rate enable** 例如：[Huawei-vlan10] **dhcp check dhcp-rate enable**	在以上 VLAN 中使能 DHCP 报文速率检查功能 缺省情况下，不使能 DHCP 报文速率检查功能，可用 **undo dhcp check dhcp-rate enable** 命令去使能对应 VLAN 中的 DHCP 报文速率检查功能
5	**dhcp check dhcp-rate** *rate* 例如：[Huawei-vlan10] **dhcp check dhcp-rate** 50	配置以上 VLAN 中的 DHCP 报文上送到 DHCP 协议栈的检查速率，超过此速率限制的 DHCP 报文会被丢弃。参数 *rate* 指定以上 VLAN 上送到 DHCP 协议栈的检查速率，取值范围为（1～100）整数个 pps 缺省情况下，未配置 DHCP 报文上送到 DHCP 协议栈的检查速率，可用 **undo dhcp check dhcp-rate** 命令恢复对应 VLAN 中的 DHCP 报文上送到 DHCP 协议栈的检查速率为缺省值
方式 3：在接口视图下配置 DHCP 报文限速		
3	**interface** *interface-type interface-number* 例如：Huawei] **interface** ethernet 2/0/0	键入要配置 DHCP 报文限速的 DHCP 服务接口，进入接口视图

（续表）

步骤	命令	说明
4	**dhcp check dhcp-rate enable** 例如：[Huawei-GigabitEthernet2/0/0]**dhcp check dhcp-rate enable**	在以上 DHCP 接口上使能 DHCP 报文速率检查功能 缺省情况下，接口视图下没有使能 DHCP 报文速率检查功能，可用 **undo dhcp check dhcp-rate enable** 命令去使能对应接口的 DHCP 报文速率检查功能
5	**dhcp check dhcp-rate** *rate* 例如：[Huawei-GigabitEthernet2/0/0] **dhcp check dhcp-rate** 10	配置以上 DHCP 接口的 DHCP 报文上送到 DHCP 协议栈的检查速率，超过此速率限制的 DHCP 报文会被丢弃。参数 *rate* 指定以上接口上送到 DHCP 协议栈的检查速率，取值范围为 1～100 整数个 pps 缺省情况下，未配置 DHCP 报文上送到 DHCP 协议栈的检查速率，可用 **undo dhcp check dhcp-rate** 命令恢复对应接口的 DHCP 报文上送到 DHCP 协议栈的检查速率为缺省值
6	**dhcp alarm dhcp-rate enable** 例如：[Huawei-GigabitEthernet2/0/0] **dhcp alarm dhcp-rate enable**	（可选）使能 DHCP 报文速率检查告警功能，如果接口下丢弃的 DHCP 报文达到告警阈值，将产生告警。但需先在对应接口视图下使用前面介绍的 **dhcp check dhcp-rate enable** 命令使能对应接口的 DHCP 报文速率检查功能 缺省情况下，不使能 DHCP 报文速率检查告警功能，可用 **undo dhcp alarm dhcp-rate enable** 命令去使能接口下 DHCP 报文速率告警功能
7	**dhcp alarm dhcp-rate threshold** *threshold* 例如：[Huawei-GigabitEthernet2/0/0] **dhcp alarm dhcp-rate threshold** 20	配置 DHCP 报文速率检查告警阈值，取值范围为 1～1 000 的整数 缺省情况下，未配置 DHCP 报文速率检查告警阈值，可用 **undo dhcp alarm dhcp-rate threshold** 命令恢复对应接口的 DHCP 报文速率检查告警阈值为缺省值 如果仅在系统视图模式下使用命令 **dhcp alarm dhcp-rate threshold** *threshold* 配置 DHCP 报文速率检查告警阈值，则接口视图下的 DHCP 报文速率检查告警阈值将和系统视图下配置的一致

5.6.2 DHCP 报文限速功能配置示例

本示例的基本网络结构如图 5-11 所示，企业某部门使用 RouterA 作为直接连接用户的设备，该部门主机作为 DHCP 客户端由 DHCP 服务器分配 IP 地址。如果出现攻击者发送大量 DHCP 报文攻击 RouterA 的情况，将会造成 RouterA 的 CPU 资源紧张，使合法用户的请求得不到及时处理。为了预防这种情况，网络管理员希望通过在 RouterA 上进行配置，对攻击者发送的 DHCP 报文进行有效防范，使合法用户的请求得到及时处理。

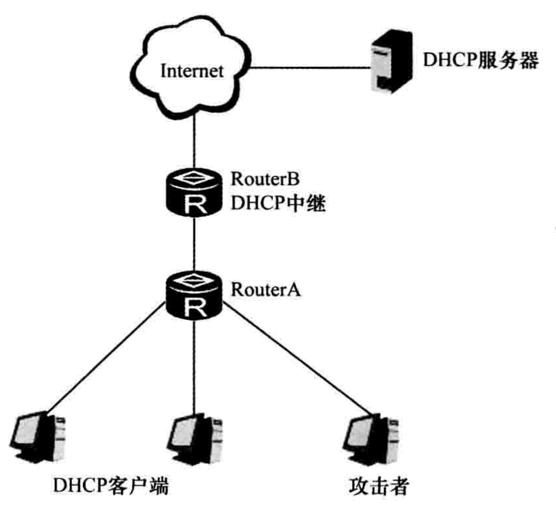


图 5-11 DHCP 报文限速配置示例的基本网络结构

本示例是要求对连接在 RouterA 上所有客户端的 DHCP 报文上传速率进行限制，故

可在 RouterA 上全局配置 DHCP 报文限速功能，实现将攻击者发送 DHCP 报文的速率限制在正常范围内的目的。具体配置步骤如下。

① 使能 DHCP 服务。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dhcp enable
```

② 配置 DHCP 报文上送速率限制。

```
[RouterA] dhcp check dhcp-rate enable        !---使能 DHCP 报文速率检查功能
[RouterA] dhcp check dhcp-rate 90            !---配置 DHCP 报文的上送速率
```

③ 配置告警功能。

```
[RouterA] dhcp alarm dhcp-rate enable        !---使能 DHCP 报文速率检查告警功能
[RouterA] dhcp alarm dhcp-rate threshold 80  !--- 配置 DHCP 报文速率检查告警阈值
```

配置好后，可通过在 RouterA 上执行 **display current-configuration | include dhcp** 命令，查看到全局情形下已经使能 DHCP 功能和 DHCP 报文限速功能（如输出信息中的粗体字显示）。

```
[RouterA] display current-configuration | include dhcp
dhcp enable
dhcp check dhcp-rate enable
dhcp check dhcp-rate 90
dhcp alarm dhcp-rate enable
dhcp alarm dhcp-rate threshold 80
```

5.7　DHCP 服务管理和典型故障排除

本节将介绍以上 DHCP 服务器地址池、DHCP 中继、DHCP 客户端的配置管理以及典型故障分析与排除方法。

5.7.1　DHCP 服务配置管理

配置好全局/接口地址池、DHCP 中继和 DHCP 客户端后，可以使用以下任意视图 **display** 命令查看配置信息，验证配置结果，或者查看 DHCP 相关报文统计信息；也用以下 **reset** 用户视图命令清除 DHCP 地址池或相关统计信息。

① **display ip pool** [**name** *ip-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]]：查看已配置的指定或全部的全局地址池信息。

② **display ip pool** [**interface** *interface-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]]：查看已配置的指定或全部接口地址池信息。

③ **display dhcp server database**：查看 DHCP 数据的存放信息。

④ **display ip pool import all**：查看路由器上配置的 DHCP 服务器自动分配给 DHCP 客户端的 DNS 等参数信息。

⑤ **display dhcp relay** { **all** | **interface** *interface-type interface-number* }：查看所有或者指定的中继接口配置的 DHCP 服务器组或服务器信息。

⑥ **display dhcp server group** [*group-name*]：查看所有或者指定的 DHCP 服务器组的配置信息。

⑦ **display this**：在对应视图下查看 DHCP/BOOTP 客户端的配置信息。

⑧ **display dhcp client**：查看开启 DHCP/BOOTP Client 接口的客户端状态信息。

⑨ **display dhcp statistics**：查看 DHCP 报文统计信息。

⑩ **display dhcp client statistics** [**interface** *interface-type interface-number*]：查看指定接口下连接的或者全部的 DHCP 客户端统计信息。

⑪ **display dhcp relay statistics** [**server-group** *group-name*]：查看所有或者指定的 DHCP 服务器组的 DHCP 中继统计信息。

⑫ **display dhcp server statistics**：查看 DHCP 服务器的统计信息。

⑬ **reset ip pool** { **interface** *interface-name* | **name** *ip-pool-name* } { *low-ip-address* [*high-ip-address*] | **all** | **conflict** | **expired** | **used** }：重置已经配置的符合指定条件的 IP 地址池。

⑭ **reset ip pool import** { **all** | **dns** | **domain-name** | **nbns** }：清除 DHCP 地址池动态获取的指定的配置参数信息。

⑮ **reset dhcp server statistics**：清除所有 DHCP 服务器的统计信息。

⑯ **reset dhcp statistics**：清除 DHCP 报文统计信息。

⑰ **reset dhcp relay statistics** [**server-group** *group-name*]：清除所有或者指定的 DHCP 服务器组的 DHCP 中继统计信息。

⑱ **reset dhcp client statistics** [**interface** *interface-type interface-number*]：清除所有或者指定接口下连接的 DHCP 客户端的统计信息。

5.7.2 典型故障分析与排除

在 DHCP 服务配置中，经常出现的两种故障是：路由器作为 DHCP 服务器或者 DHCP 中继时，DHCP 客户端无法获取 IP 地址。下面分别介绍这两种情形下的故障排除方法。

1. 设备作为 DHCP 服务器时，DHCP 客户端无法动态获取 IP 地址

下面是具体的排除步骤。

（1）执行 **display current-configuration | include dhcp enable** 命令，检查 DHCP 功能是否已经使能。**缺省情况下，DHCP 功能未使能。**

① 如果无任何 DHCP 相关显示信息，说明 DHCP 功能未使能，可在系统视图下执行 **dhcp enable** 命令使能 DHCP 功能。

② 如果显示了“dhcp enable”，说明 DHCP 功能已经使能，则继续以下检查。

（2）在接口视图下，执行 **display this** 命令检查是否选择了 DHCP 分配地址的方式。

① 如果显示的是“dhcp select global”，则表明接口已经选择全局地址池为 DHCP 客户端分配 IP 地址，这时请继续下面的步骤（3）。

② 如果显示的是“dhcp select interface”，则表明接口已经选择接口地址池为 DHCP 客户端分配 IP 地址，这时请继续下面的步骤（4）。

③ 如果无上述显示信息，则表明接口没有选择 DHCP 分配地址的方式，则需要在对应的接口视图下配置 **dhcp select global** 或者 **dhcp select interface** 命令，配置接口选择全局或者接口地址池的 IP 地址分配方式。

（3）执行命令 **display ip pool**，查看全局地址池是否存在。

① 如果全局地址池不存在，则要使用 **ip pool** *ip-pool-name* 和 **network** *ip-address* [**mask** { *mask* | *mask-length* }] 命令创建全局地址池。

② 如果全局地址池存在，可通过执行 **display ip pool** name *ip-pool-name* 命令查看全局地址池中的 IP 地址是否与接口的 IP 地址在同一个网段中。

a. 如果 DHCP 客户端与 DHCP 服务器在同一个网段内（中间没有中继设备）。

- 如果全局地址池中的 IP 地址与连接 DHCP 客户端的路由器接口的 IP 地址不在同一个网段中，则执行 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] 命令修改接口的 IP 地址，使二者在一个网段中。
- 如果全局地址池中的 IP 地址与连接 DHCP 客户端的路由器接口的 IP 地址在同一个网段中，则继续下面的步骤（4）。

b. 如果 DHCP 客户端与 DHCP 服务器不在同一个网段内（中间存在中继设备）。

- 如果连接 DHCP 中继的路由器接口的 IP 地址与中继设备接口的 IP 地址不在同一个网段中，则执行 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] 命令修改接口的 IP 地址，使二者在一个网段中。
- 如果连接 DHCP 中继的路由器接口的 IP 地址与中继设备接口的 IP 地址在同一个网段中，请继续下面的步骤（4）。

（4）执行 **display ip pool** [{ **interface** *interface-pool-name* | **name** *ip-pool-name* } [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]] 命令，检查全局/接口地址池中 IP 地址使用情况。当其中的 **"Idle（Expired）"** 值等于 0 时，说明地址池中的 IP 地址已经用尽。

① 如果接口选择全局地址池为 DHCP 客户端分配 IP 地址，可以重新创建一个全局地址池，该地址池的网段不能和前一个地址池的网段重叠，但网段可以相连。

② 如果 DHCP 服务器选择接口地址池为 DHCP 客户端分配 IP 地址，用户可以配置缩小接口地址掩码长度，从而扩大可分配的 IP 地址范围。

2. 设备作为 DHCP 中继时，DHCP 客户端无法获取 IP 地址

下面是具体的排除步骤。

（1）执行**display current-configuration** | **include dhcp enable** 命令，检查 DHCP 功能是否已经使能。缺省情况下，DHCP 功能未使能。

① 如果无任何显示信息，说明 DHCP 功能未使能，执行 **dhcp enable** 命令使能 DHCP 功能。

② 如果显示 **dhcp enable**，说明 DHCP 功能已经使能。

（2）在 DHCP 中继接口视图下，执行 **display this** 命令检查 DHCP 中继是否处于使能状态。

① 如果显示 **dhcp select relay**，说明 DHCP 中继已经处于使能状态，请继续下面的步骤 3。

② 如果无上述显示信息，说明 DHCP 中继处于未使能状态，执行 **dhcp select relay** 命令，使能 DHCP 中继功能。

（3）同样，在 DHCP 中继接口视图下，执行 **display this** 命令，检查 DHCP 中继是

否配置了所代理的 DHCP 服务器。

① 如果显示 **dhcp relay server-ip** *ip-address*，说明 DHCP 中继已经配置了所代理的 DHCP 服务器。

② 如果显示 **dhcp relay server-select** *group-name*，说明 DHCP 中继接口绑定了 DHCP 服务器组，则继续下面的步骤（4）。

③ 如果无上述显示信息，说明 DHCP 中继没有配置 DHCP 服务器，请从以下两种配置方法中选择一种来配置 DHCP 服务器。

- 配置 **dhcp relay server-ip** *ip-address* 系统视图命令，配置 DHCP 中继所代理的 DHCP 服务器地址。
- 配置 **dhcp server group** *group-name* 系统视图命令，创建 DHCP 服务器组，然后配置 **dhcp-server** *ip-address* [*ip-address-index*]系统视图命令，在 DHCP 服务器组中添加 DHCP 服务器；并执行 **dhcp relay server-select** *group-name* 系统视图命令，绑定 DHCP 服务器组。

（4）执行 **display dhcp server group** *group-name* 命令，检查 DHCP 服务器组中是否配置了 DHCP 服务器。

① 如果显示 **Server-IP** 字段，说明 DHCP 服务器组中配置了 DHCP 服务器。

② 如果无上述显示字段，说明 DHCP 服务器组中没有配置 DHCP 服务器，请执行 **dhcp-server** *ip-address* [*ip-address-index*]命令，在 DHCP 服务器组中添加 DHCP 服务器。

5.8 DHCP Snooping 基础

DHCP Snooping 是一种 DHCP 安全技术，能够有效防止网络中仿冒 DHCP 服务器的攻击，保证客户端从合法的服务器获取 IP 地址，而且能够记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系进而生成绑定表，同时还可以防范各种基于 DHCP 服务的攻击。

说明 AR150/150-S/160/200/200-S/1200/1200-S 系列产品不支持 DHCP Snooping 功能，4GE-2S、4ES2G-S、4ES2GP-S 和 9ES2 单板也不支持 DHCP Snooping 功能。

5.8.1 DHCP Snooping 概述

目前，DHCP 协议在应用的过程中遇到很多安全方面的问题，网络中存在一些针对 DHCP 的各种攻击，如 DHCP 服务器仿冒者攻击、DHCP 服务器拒绝服务攻击、仿冒 DHCP 报文攻击等。

为了保证网络通信业务的安全性，引入了 DHCP Snooping 技术。DHCP Snooping 是 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系，防止网络上针对 DHCP 服务的攻击。

DHCP Snooping 能够实现“信任功能”和“基本侦听功能”。下面分别予以介绍。

1. 信任功能

网络中如果存在私自架设的伪 DHCP 服务器，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。DHCP Snooping 的信任功能可以控制 DHCP 服务器应答报文的来源，防止网络中可能存在的伪造或非法 DHCP 服务器为其他主机分配 IP 地址及其他配置信息。

DHCP Snooping 信任功能允许将端口分为信任端口和非信任端口。

① 信任端口正常转发接收到的 DHCP 应答报文。

② 非信任端口在接收到 DHCP 服务器响应的 DHCP Ack、DHCP Nak 和 DHCP Offer 报文后，丢弃该报文。

管理员在部署网络时，一般将直接或间接连接合法 DHCP 服务器的端口设置为信任端口，其他端口设置为非信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，而私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2. 基本侦听功能

出于安全性的考虑，管理员需要记录用户上网时所用的 IP 地址，确认用户申请的 IP 地址和用户使用主机的 MAC 地址的对应关系。开启 DHCP Snooping 功能后，设备能够通过侦听 DHCP 请求报文和回应报文，生成 DHCP Snooping 绑定表。绑定表项包括客户端的 MAC 地址、获取到的 IP 地址、与 DHCP 客户端连接的端口及该端口所属的 VLAN 等信息。即 DHCP Snooping 绑定表记录了 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系。

通过对所接收的 DHCP 报文与 DHCP Snooping 绑定表进行匹配检查，就能够有效地防止攻击者构造合法用户报文对网络进行的攻击。另外，DHCP Snooping 绑定表还可根据各用户 IP 地址的 DHCP 租用期进行老化，或根据用户释放 IP 地址时发出的 DHCP Release 报文自动删除对应表项。

在设备通过 DHCP Snooping 功能生成绑定表后，管理员可以方便地记录 DHCP 用户申请的 IP 地址与所用主机的 MAC 地址之间的对应关系。但在通过 DHCP Snooping 的基本侦听功能生成绑定表的过程中，为了保证设备能够获取用户 MAC 地址等参数，DHCP Snooping 功能需应用于二层接入设备或第一个 DHCP 中继上。

5.8.2 DHCP Snooping 支持的 Option82 功能

在传统的 DHCP 动态分配 IP 地址过程中，DHCP 服务器不能根据 DHCP 请求报文感知到用户的具体物理位置，以致同一 VLAN 的用户得到的 IP 地址所拥有的权限是完全相同的，这就不能对同一 VLAN 中特定的用户进行有效的控制。

RFC 3046 定义了 DHCP Relay Agent Information Option（DHCP 中继代理信息选项，即 Option 82），该选项记录了 DHCP 客户端的位置信息。DHCP Snooping 设备或 DHCP 中继通过在 DHCP 请求报文中添加 Option82 选项，将 DHCP 客户端的精确物理位置信息传递给 DHCP 服务器，从而使得 DHCP 服务器能够为主机分配合适的 IP 地址和其他配置信息，实现对客户端的安全控制。

Option82 包含两个子选项 Circuit ID（Sub-option 1）和 Remote ID（Sub-option 2）。

其中 Circuit ID 子选项主要用来标识客户端所在的 VLAN、端口等信息，Remote ID 子选项主要用来标识客户端接入的设备，一般为设备的 MAC 地址。这方面内容请参见 5.1.5 小节。

说明 设备作为 DHCP 中继时，使能或未使能 DHCP Snooping 功能都可支持 Option82 选项功能，但若设备在二层网络作为接入设备，则必须使能 DHCP Snooping 功能方可支持 Option82 功能。Option82 选项仅记录了 DHCP 用户的精确物理位置信息并通过 DHCP 请求报文将该信息发送给 DHCP 服务器。而如果需要对不同的用户部署不同的地址分配或安全策略，则需 DHCP 服务器支持 Option82 功能并在其上已配置了 IP 地址分配或安全策略。

Option82 选项携带的用户位置信息与 DHCP Snooping 绑定表记录的用户参数是两个相互独立的概念，没有任何关联。Option82 选项携带的用户位置信息是在 DHCP 用户申请 IP 地址时（此时用户还未分配到 IP 地址），由设备添加到 DHCP 请求报文中。DHCP Snooping 绑定表中的位置信息是在设备收到 DHCP 服务器回应的 DHCP Ack 报文时（此时已为用户分配了 IP 地址），设备根据 DHCP Ack 报文信息自动生成。

设备作为 DHCP 中继或设备在二层网络作为接入设备并使能 DHCP Snooping 功能时均可支持 Option82 功能。使能设备的 Option82 功能有 Insert 和 Rebuild 两种方式，使能方式不同，设备对报文的处理也不同。

① Insert 方式：当设备收到 DHCP 请求报文时，若该报文中没有 Option82 选项，则插入 Option82 选项；若该报文中含有 Option82 选项，则判断 Option82 选项中是否包含 remote-id，如果包含，则保持 Option82 选项不变，如果不包含，则插入 remote-id。

② Rebuild 方式：当设备收到 DHCP 请求报文时，若该报文中没有 Option82 选项，则插入 Option82 选项；若该报文中含有 Option82 选项，则删除该 Option82 选项并插入管理员自己在设备上配置的 Option82 选项。

对于 Insert 和 Rebuild 两种方式，当设备接收到 DHCP 服务器的响应报文时，处理方式一致：若该报文中含有 Option82 选项，则删除之，并转发给 DHCP 客户端；若报文中不含有 Option82 选项，则直接转发。

5.8.3 DHCP Snooping 的典型应用

DHCP Snooping 功能的主要应用体现以在以下几个方面。

- 防止 DHCP 服务器仿冒者攻击。
- 防止非 DHCP 用户攻击。
- 防止 DHCP 报文泛洪攻击。
- 防止仿冒 DHCP 报文攻击。
- 防止 DHCP 服务器拒绝服务攻击。
- 通过 Option82 的支持实现对 DHCP 客户端的安全控制。

下面分别介绍这几种应用。

1. 防止 DHCP 服务器仿冒者攻击

由于 DHCP 服务器和 DHCP 客户端之间没有认证机制，所以如果在网络上随意

添加一台 DHCP 服务器，它就可以为客户端分配 IP 地址以及其他网络参数。如果该 DHCP 服务器为用户分配错误的 IP 地址和其他网络参数，将会对网络造成非常大的危害。

如图 5-12 所示，DHCP 客户端发送的 DHCP Discover 报文是以广播形式发送的，无论是合法的 DHCP 服务器，还是非法的 DHCP 服务器都可以接收到。如果此时 DHCP 服务器仿冒者回应给 DHCP 客户端仿冒信息，如错误的网关地址、错误的 DNS 服务器、错误的 IP 等信息，如图 5-13 所示，DHCP 客户端将无法获取正确的 IP 地址和相关信息，导致合法客户无法正常访问网络或信息安全受到严重威胁。

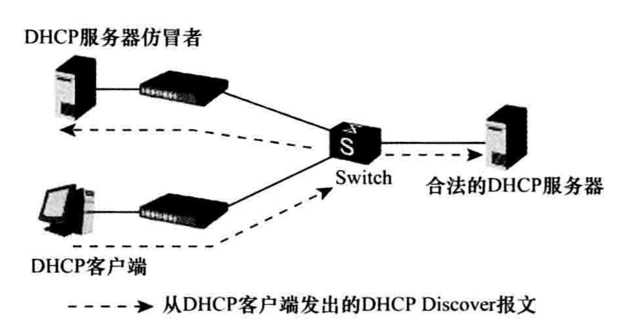


图 5-12　DHCP 客户端发送 DHCP Discover 报文示意图

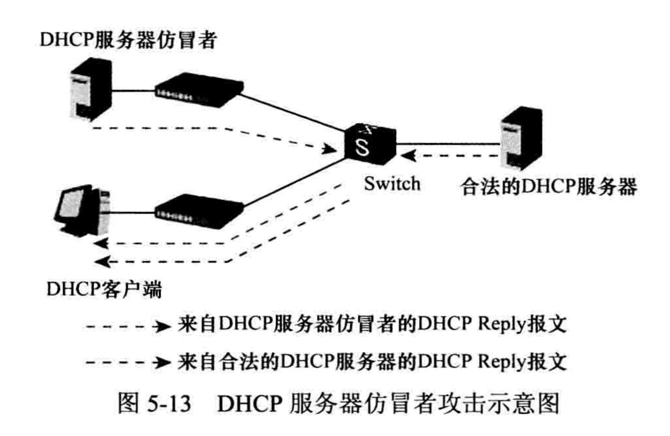


图 5-13　DHCP 服务器仿冒者攻击示意图

为了防止这种 DHCP 服务器仿冒者攻击，可配置设备接口的“信任（Trusted）/非信任（Untrusted）”工作模式，将与合法 DHCP 服务器直接或间接连接的端口设置为信任端口，其他端口设置为非信任端口。此后，从“非信任（Untrusted）”端口上收到的 DHCP 回应报文将被直接丢弃，这样可以有效防止 DHCP 服务器仿冒者的攻击。

2. 防止非 DHCP 用户攻击

在 DHCP 网络中，静态获取 IP 地址的用户（非 DHCP 用户）对网络可能存在多种攻击，譬如仿冒 DHCP 服务器、构造虚假 DHCP Request 报文等。这将为合法 DHCP 用户正常使用网络带来一定的安全隐患。

为了有效地防止这种非 DHCP 用户攻击，可开启设备根据 DHCP Snooping 绑定表生成接口的静态 MAC 表项功能。之后，设备将根据接口下所有的 DHCP 用户对应的 DHCP Snooping 绑定表项自动执行命令生成这些用户的静态 MAC 表项，并同时关闭接口学习

动态 MAC 表项的能力。此时，只有源 MAC 地址与静态 MAC 表项匹配的报文才能够通过该接口，否则报文会被丢弃。因此对于该接口下的非 DHCP 用户，只有管理员手动配置了此类用户的静态 MAC 表项其报文才能通过，否则报文将被丢弃。

3. 防止 DHCP 报文泛洪攻击

在 DHCP 网络环境中，若攻击者短时间内向设备发送大量的 DHCP 报文，将会对设备的性能造成巨大的冲击以致可能会导致设备无法正常工作。

为了有效地防止这种 DHCP 报文泛洪攻击，在使能设备的 DHCP Snooping 功能时，可同时使能设备对 DHCP 报文上送 DHCP 报文处理单元的速率进行检测的功能。此后，设备将会检测 DHCP 报文的上送速率，并仅允许在规定速率内的报文上送至 DHCP 报文处理单元，而超过规定速率的报文将会被丢弃。

4. 防止仿冒 DHCP 报文攻击

在 DHCP 服务提供过程中，已获取到 IP 地址的合法用户通过向服务器发送 DHCP Request 或 DHCP Release 报文续租或释放 IP 地址。如果攻击者冒充合法用户不断向 DHCP 服务器发送 DHCP Request 报文来续租 IP 地址，会导致这些到期的 IP 地址无法正常回收，以致一些合法用户不能获得 IP 地址；而若攻击者仿冒合法用户的 DHCP Release 报文发往 DHCP 服务器，会导致用户异常下线。

为了有效地防止这种仿冒 DHCP 报文攻击，可使用 DHCP Snooping 绑定表的功能。设备通过将 DHCP Request 续租报文和 DHCP Release 报文与绑定表进行匹配操作能够有效地判别报文是否合法，若匹配成功则转发该报文，匹配不成功则丢弃。

5. 防止 DHCP 服务器拒绝服务攻击

如果设备某接口下存在大量攻击者恶意申请 IP 地址，会导致 DHCP 服务器中 IP 地址快速耗尽而不能为其他合法用户提供 IP 地址分配服务。另一方面，DHCP 服务器通常仅根据 DHCP Request 报文中的 chaddr 字段来确认客户端的 MAC 地址。如果某一攻击者通过不断改变 Chaddr 字段向 DHCP 服务器申请 IP 地址，同样将会导致 DHCP 服务器上的地址池被耗尽，从而无法为其他正常用户提供 IP 地址。

为了抑制大量 DHCP 用户恶意申请 IP 地址，在使能设备的 DHCP Snooping 功能后，可配置设备或接口允许接入的最大 DHCP 用户数，当接入的用户数达到该值时，则不再允许任何用户通过此设备或接口成功申请到 IP 地址。而对通过改变 DHCP Request 报文中的 Chaddr 字段方式的攻击，可使能设备检测 DHCP Request 报文帧头 MAC 地址与 DHCP 数据区中 Chaddr 字段是否一致功能，此后设备将检查上送的 DHCP Request 报文中的帧头 MAC 地址是否与 Chaddr 值相等，相等则转发，否则丢弃。

6. 通过支持的 Option82 实现对客户端的安全控制

Option82 称为中继代理信息选项，该选项记录了 DHCP 客户端的位置信息。DHCP Snooping 设备或 DHCP 中继通过在 DHCP 请求报文中添加 Option82 选项，将 DHCP 客户端的位置信息传递给 DHCP 服务器，从而使得 DHCP 服务器能够为主机分配合适的 IP 地址和其他配置信息，并实现对客户端的安全控制。

如图 5-14 所示，用户通过 DHCP 方式获取 IP 地址。在管理员组建该网络时需要控制接口 interface1 下用户对网络资源的访问以提高网络的安全性。在传统的 DHCP 动态分配 IP 地址过程中，DHCP 服务是无法区分同一 VLAN 内的不同用户的，以致同一 VLAN

内的用户得到的 IP 地址所拥有的权限是完全相同的。

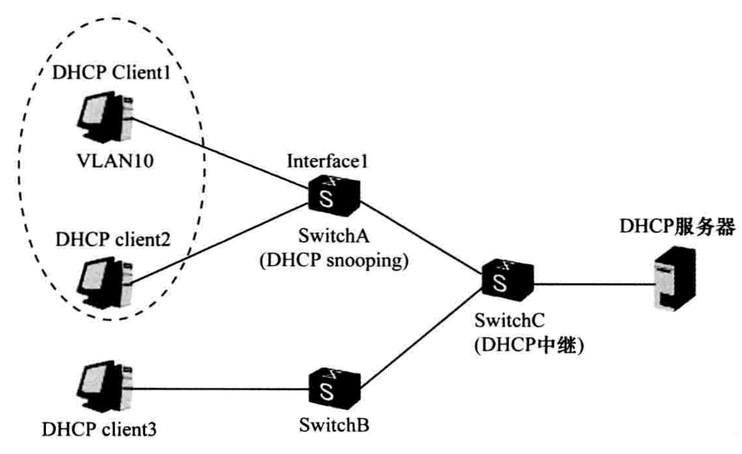


图 5-14 通过 Option82 的支持实现对客户端安全控制的示例

为实现上述目的，管理员在使能 SwitchA 的 DHCP Snooping 功能之后可使能其 Option82 功能。之后 SwitchA 在接收到用户申请 IP 地址发送的 DHCP Request 报文时，会在报文中插入 Option82 选项，以标注用户的精确位置信息，譬如 MAC 地址、所属 VLAN、所连接的端口号等参数。DHCP 服务器在接收到携带有 Option82 选项的 DHCP 请求报文后，即可通过 Opion82 选项的内容获悉用户的精确物理位置进而根据其上已部署的 IP 地址分配策略或其他安全策略为用户分配合适的 IP 地址和其他配置信息。

5.9 DHCP Snooping 的基本功能配置与管理

DHCP Snooping 的基本功能就是能够保证客户端从合法的服务器获取 IP 地址，而且能够记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系进而生成绑定表。

DHCP Snooping 的基本功能的配置任务如下（**只有前面两项是必选的**）。

① 使能 DHCP Snooping 功能。

② 配置接口信任状态。

③（可选）使能 DHCP Snooping 用户位置迁移功能。

④（可选）配置 ARP 与 DHCP Snooping 的联动功能。

⑤（可选）配置用户下线后及时清除对应 MAC 表项功能。

⑥（可选）配置丢弃 GIADDR 字段非零的 DHCP Request 报文。

5.9.1 使能 DHCP Snooping 功能

在配置 DHCP Snooping 各安全功能之前需首先使能 DHCP Snooping 功能。使能 DHCP Snooping 功能的配置顺序是先使能全局下的 DHCP Snooping 功能，再使能接口或 VLAN 下的 DHCP Snooping 功能，具体配置步骤如表 5-15 所示。

表 5-15 使能 **DHCP Snooping** 功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**dhcp snooping enable** 例如：[Huawei]**dhcp snooping enable**	全局使能 DHCP Snooping 功能 缺省情况下，设备全局未使能 DHCP Snooping 功能，可用 **undo dhcp snooping enable** 命令去使能全局 DHCP Snooping 功能
3	**vlan** *vlan-id* 例如：[Huawei] **vlan** 2	（二选一）键入要使能 DHCP Snooping 功能的 VLAN，进入 VLAN 视图
	interface *interface-type interface-number* 例如：[Huawei] **interface** ethernet 2/0/0	（二选一）键入要使能 DHCP Snooping 功能的物理接口，进入接口视图
4	**dhcp snooping enable** 例如：[Huawei-vlan2] **dhcp snooping enable** 或者[Huawei-Ethernet2/0/0]**dhcp snooping enable**	使能以上 VLAN 或接口下的 DHCP Snooping 功能。在 VLAN 视图下执行此命令，则对设备所有接口接收到的属于该 VLAN 的 DHCP 报文命令功能生效。 缺省情况下，设备未使能 DHCP Snooping 功能，可用 **undo dhcp snooping enable** 命令去使能对应 VLAN 或者接口的 DHCP Snooping 功能 【说明】在系统视图下使用 **dhcp snooping enable** vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10> 命令配置，在功能上与在 VLAN 视图下执行命令 **dhcp snooping enable** 相同，而且这样还可以一次性为多个 VLAN 使能 DHCP Snooping 功能。 但如果使用 **dot1q termination vid** 命令配置了子接口 dot1q 封装的单层 VLAN ID，则不能在该 VLAN 内使能 DHCP Snooping 功能

5.9.2 配置接口信任状态

为使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，需将与信任的 DHCP 服务器直接或间接连接的设备接口设置为信任接口，其他接口设置为非信任接口。其中，信任接口正常转发接收到的 DHCP 应答报文；非信任接口在接收到 DHCP 服务器响应的 DHCP Ack、DHCP Nak 和 DHCP Offer 报文后，丢弃该报文。这样就可以保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

在连接用户的接口或 VLAN 下使能 DHCP Snooping 功能之后，需将连接 DHCP 服务器的接口配置为“信任”模式，两者同时生效的设备才能够生成 DHCP Snooping 动态绑定表。

配置接口信任状态，可在接口视图或 VLAN 视图下执行。具体配置步骤如表 5-16 所示。

表 5-16 接口信任状态的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
方式 1：在接口下配置接口信任状态		
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** ethernet 2/0/0	键入要配置为信任状态的接口（通常所直接或间接连接 DHCP 服务器的接口），进入接口视图
3	**dhcp snooping trusted** 例如：[Huawei-Ethernet2/0/0] **dhcp snooping trusted**	配置以上接口为“信任”接口 缺省情况下，接口的状态为“非信任”状态，可用 **undo dhcp snooping trusted** 命令恢复以上接口为非信任状态
方式 2：在 VLAN 下配置接口信任状态		
2	**vlan** *vlan-id* 例如：[Huawei] **vlan** 2	键入要配置信任接口的 VLAN，进入 VLAN 视图
3	**dhcp snooping trusted interface** *interface-type interface-number* 例如：[Huawei-vlan2] **dhcp snooping trusted interface** ethernet 2/0/0	配置指定接口为 VLAN 中的“信任”接口。参数 *interface-type interface-number* 用来指定要配置为信任状态的接口 缺省情况下，接口的状态为“非信任”状态，可用 **undo dhcp snooping trusted interface** *interface-type interface-number* 命令恢复指定接口为非信任状态

5.9.3 使能 DHCP Snooping 用户位置迁移功能

在移动应用场景中，若某一用户由接口 A 上线，然后要切换到接口 B，这时为了让用户能够上线，需要使能 DHCP Snooping 用户位置迁移功能。

使能 DHCP Snooping 用户位置迁移功能的配置方法很简单，仅需在系统视图下执行 **dhcp snooping user-transfer enable** 命令，使用户切换了所连接的交换机接口后仍能保持网络连接。

缺省情况下，已使能 DHCP Snooping 用户位置迁移功能，可用 **undo dhcp snooping user-transfer enable** 命令去使能 DHCP Snooping 用户位置迁移功能。

5.9.4 配置 ARP 与 DHCP Snooping 的联动功能

DHCP Snooping 设备在收到 DHCP 用户发出的 DHCP Release 报文时会删除该用户对应的绑定表项，但若用户发生了异常下线而无法发出 DHCP Release 报文时，DHCP Snooping 设备将不能及时地删除该 DHCP 用户对应的绑定表。

使能 ARP 与 DHCP Snooping 的联动功能后，如果 DHCP Snooping 表项中的 IP 地址对应的 ARP 表项达到老化时间，则 DHCP Snooping 设备会对该 IP 地址进行 ARP 探测，如果在规定的探测次数内探测不到用户，设备将删除用户对应的 ARP 表项。之后，设备会再次按规定的探测次数对该 IP 地址进行 ARP 探测，如果最后仍不能够探测到用户，则设备会删除该用户对应的绑定表项。**但只有当设备作为 DHCP 中继时，才支持 ARP 与 DHCP Snooping 的联动功能。**

使能 ARP 与 DHCP Snooping 的联动功能的配置方法也很简单，仅需在系统视图下执行 **arp dhcp-snooping-detect enable** 命令。使能后，系统会周期性地对该 IP 地址进行

ARP 探测，如果在规定的探测次数内（探测次数的配置命令为 **arp detect-times** *detect-times*）探测不到用户，则系统会删除 DHCP 绑定表表项，并且构造 Release 报文通知 DHCP 服务器，释放 IP 地址；如果查询不到用户 ARP 表项，会发送 ARP 报文探测用户，网络上的 ARP 报文流量会增加。

缺省情况下，设备没有使能 ARP 与 DHCP Snooping 的联动功能，可用 **undo arp dhcp-snooping-detect enable** 命令去使能 ARP 与 DHCP Snooping 的联动功能。

5.9.5 配置用户下线后及时清除对应 MAC 表项功能

当某一 DHCP 用户下线时，若 DHCP 服务器或者 DHCP 中继设备上其对应的动态 MAC 表项还未达到老化时间，则设备在接收到来自网络侧以该用户 IP 地址为目的地址的报文时，将继续根据动态 MAC 表项转发此报文，当然最终结果没有成功，因为该用户已下线了。但这种无效的报文处理在一定程度上会降低设备的性能。

根据 DHCP 服务的工作原理可知，当 DHCP 服务器或者 DHCP 中继设备在接收到 DHCP 用户下线时发送 DHCP Release 报文后，会立刻删除用户对应的 DHCP Snooping 绑定表项。利用这种特性，就可使能设备在 DHCP Snooping 动态表项被清除的同时，删除对应用户的 MAC 表项功能。这样当用户下线时，设备会及时地删除该用户的 MAC 表项。

使能当 DHCP Snooping 动态表项清除时移除对应用户的 MAC 表项功能的配置方法同样很简单，仅需在系统视图下执行 **dhcp snooping user-offline remove mac-address** 命令。缺省情况下，未使能当 DHCP Snooping 动态表项清除时移除对应用户的 MAC 表项功能，可用 **undo dhcp snooping user-offline remove mac-address** 命令去使能当 DHCP snooping 表项清除时移除对应用户的 MAC 表项功能。

5.9.6 配置丢弃 GIADDR 字段非零的 DHCP Request 报文

DHCP 请求报文中的 GIADDR（网关 IP 地址）字段记录了 DHCP 请求报文经过的第一个 DHCP 中继的 IP 地址。正常情况下，当客户端发出 DHCP 请求时，如果 DHCP 服务器和客户端不在同一个网段，那么第一个 DHCP 中继在将 DHCP 请求报文转发给 DHCP 服务器前把自己的 IP 地址填入 Giaddr 字段中。DHCP 服务器在收到 DHCP 请求报文后，会根据 Giaddr 字段值来判断出客户端所在的网段地址，从而选择合适的地址池，为客户端分配该网段的 IP 地址。

然而，在通过 DHCP Snooping 的基本侦听功能生成绑定表的过程中，为了保证设备能够获取到客户端 MAC 地址等参数，DHCP Snooping 功能需应用于二层接入设备或第一个 DHCP 中继上。此时，在 DHCP Snooping 设备接收到的 DHCP 请求报文中 Giaddr 字段必然为 0.0.0.0，如果不为 0.0.0.0，则为非法报文，需丢弃此类报文。

可在 VLAN 视图或者接口视图下通过 **dhcp snooping check dhcp-giaddr enable** 命令使能检测 DHCP 请求报文中 GIADDR 字段是否非零的功能。当在 VLAN 视图下配置时，则对 DHCP Snooping 设备上所有接口在接收到的属于该 VLAN 的 DHCP 请求报文时都要进行 Giaddr 字段是否非零的检测，而在接口视图下配置时，仅对对应接口上收到的 DHCP 请求报文进行 Giaddr 字段是否非零的检测。

缺省情况下，若未使能检测 DHCP Request 报文中 Giaddr 字段是否非零的功能，可用 **undo dhcp snooping check dhcp-giaddr enable** 命令去使能对应 VLAN 或者接口下检测 DHCP Request 报文中 Giaddr 字段是否非零的功能。

5.9.7 DHCP Snooping 基本功能管理

在配置完成 DHCP Snooping 的基本功能后，可通过以下 **display** 任意视图命令查看相关配置信息，验证配置结果；也可以使用以下 **reset** 用户视图命令清除相关统计信息。

① **display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]：查看指定接口或全部接口的 DHCP Snooping 运行信息。

② **display dhcp snooping configuration** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]：查看指定 VLAN 或者指定接口或者全部的 DHCP Snooping 配置信息。

③ **display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*| **vlan** *vlan-id* } * | **all** } [**verbose**]：查看指定接口、IP 地址、MAC 地址、VLAN 或者所有 DHCP Snooping 绑定表信息。

④ **reset dhcp snooping statistics global**：清除全局的报文丢弃统计计数。

⑤ **reset dhcp snooping statistics interface** *interface-type interface-number* [**vlan** *vlan-id*]：清除指定接口下指定 VLAN 或者所有 VLAN 中的报文丢弃统计计数。

⑥ **reset dhcp snooping statistics vlan** *vlan-id* [**interface** *interface-type interface-number*]：清除指定 VLAN 下指定接口或者所有接口的报文丢弃统计计数。

⑦ **reset dhcp snooping user-bind** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] *：清除指定 VLAN、指定接口或者所有 DHCP Snooping 动态绑定表。

5.10 DHCP Snooping 的攻击防范功能配置与管理

在配置完成 DHCP Snooping 的基本功能后，设备能够保证客户端从合法的服务器获取 IP 地址，这有效防止了网络中 DHCP Server 仿冒者攻击。但是在 DHCP 网络环境中，攻击者仍有多种攻击手段可对网络进行攻击。此时根据需要，管理员可配置 DHCP Snooping 的攻击防范功能。

配置 DHCP Snooping 的攻击防范功能之前，务必确保已完成 DHCP Snooping 的基本功能配置。主要包括以下三项配置任务，可根据实际需要选择配置。

① 配置防止 DHCP 服务器仿冒者攻击。

② 配置防止仿冒 DHCP 报文攻击。

③ 配置防止 DHCP 服务器拒绝服务攻击。

5.10.1 配置防止 DHCP 服务器仿冒者攻击

通过配置 DHCP 服务器探测功能，DHCP Snooping 设备会检查并在日志中记录所有 DHCP 应答（DHCP Reply）报文中携带的 DHCP 服务器地址与端口等信息，此后网络管理员可根据日志来判定网络中是否存在伪 DHCP 服务器进而对网络进行维护。

说明 日志文件名由系统自动生成，其后缀是“*.log”或者“*.dblg”，可用 **display logfile** *file-name* 任意视图命令查看日志文件，也可用 **display logbuffer** 任意视图命令查看 Log 缓冲区记录的日志信息。

DHCP 服务器探测功能的方法很简单，仅须在系统视图下执行 **dhcp server detect** 命令即可。但在执行本命令之前，需确保已使用 **dhcp snooping enable** 命令使能了设备的 DHCP Snooping 功能。

缺省情况下，未使能 DHCP Server 探测功能，需要时（如网络中很安全，不存在仿冒 DHCP 服务器）可用 **undo dhcp server detect** 命令去使能 DHCP Server 探测功能。

5.10.2 配置防止仿冒 DHCP 报文攻击

在 DHCP 网络环境中，如果攻击者仿冒合法用户的 DHCP Request 报文并发往 DHCP 服务器，将导致合法用户的 IP 地址租约到期之后不能及时释放，也无法使用该 IP 地址；如果攻击者仿冒合法用户的 DHCP Release 报文发往 DHCP 服务器，又将导致合法用户异常下线。使能了 DHCP Snooping 功能后，设备可根据生成的 DHCP Snooping 绑定表项，对 DHCP Request 报文或 DHCP Release 报文进行匹配检查，只有匹配成功的报文设备才将其转发，否则将丢弃。这可有效地防止非法用户通过发送伪造 DHCP Request 或 DHCP Release 报文冒充合法用户续租或释放 IP 地址。

DHCP Snooping 设备对 DHCP Request 报文或 DHCP Release 报文的匹配检查规则如下。

（1）对 DHCP Request 报文

① 首先检查报文的目的 MAC 地址是否是为全 F，如果是，则认为是第一次上线的 DHCP Request 广播报文，直接通过；如果报文的目的 MAC 地址不是全 F，则认为是续租报文，将根据绑定表项对报文中的 VLAN、IP 地址、接口信息进行匹配检查，完全匹配才通过。

② 检查报文中的 CHADDR 字段值是否与绑定表中的网关地址匹配，如果不匹配，则认为是用户第一次上线，直接通过；如果匹配，则继续检查报文中的 VLAN、IP 地址、接口信息是否均和绑定表匹配，完全匹配通过，否则丢弃。

（2）对 DHCP Release 报文

将直接检查报文中的 VLAN、IP 地址、MAC 地址、接口信息是否匹配绑定表，匹配则通过，不匹配则丢弃。

防止仿冒 DHCP 报文攻击的配置步骤如表 5-17 所示。

表 5-17 防止仿冒 DHCP 报文攻击的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
使能对 DHCP 报文进行绑定表匹配检查的功能（**可在 VLAN 视图或者接口视图下配置**）		
2	**vlan** *vlan-id* 例如：[Huawei] **vlan** 10	（二选一）键入要使能对 DHCP 报文进行绑定表匹配检查的功能的 VLAN，进入 VLAN 视图
	interface *interface-type interface-number* 例如：[Huawei] **interface** ethernet 2/0/0	（二选一）键入要使能对 DHCP 报文进行绑定表匹配检查的功能的接口，进入接口视图

（续表）

步骤	命令	说明
3	**dhcp snooping check user-bind enable** 例如：[Huawei-vlan10] **dhcp snooping check user-bind enable** 或 [Huawei-Ethernet2/0/0] **dhcp snooping check user-bind enable**	使能对 DHCP 报文进行绑定表匹配检查的功能 在 VLAN 视图下执行此命令，则对 DHCP Snooping 设备上所有接口接收到的属于该 VLAN 的 DHCP 报文都将进行绑定表匹配检查 缺省情况下，未使能对 DHCP 报文进行绑定表匹配检查功能，可用 **undo dhcp snooping check user-bind enable** 命令去使能该功能
使能 DHCP Snooping 告警功能（**仅可在接口视图下配置**）		
4	**dhcp snooping alarm user-bind enable** 例如：[Huawei-Ethernet2/0/0] **dhcp snooping alarm user-bind enable**	使能与绑定表不匹配而被丢弃的 DHCP 报文数达到阈值时的 DHCP Snooping 告警功能。使能告警功能后如果有对应的攻击，并且丢弃的攻击报文超过阈值，会有相应的告警信息出现。发送告警的最小时间间隔为 1 min。 缺省情况下，未使能 DHCP Snooping 告警功能，可用 **undo dhcp snooping alarm enable** 命令去使能该功能
配置 DHCP Snooping 丢弃报文数量的告警阈值（**可在系统视图或接口视图下配置**）		
5	**dhcp snooping alarm threshold** *threshold* 例如：[Huawei] **dhcp snooping alarm threshold** 50	（可多选）在系统视图下配置 DHCP Snooping 丢弃报文的告警阈值（当设备丢弃的**所有类型报文数**达到阈值时将会告警），取值范围是 1～1 000 的整数 缺省情况下，全局情况下，DHCP Snooping 丢弃报文数量的告警阈值为 100 个包，可用 **undo dhcp snooping alarm threshold** 命令恢复全局告警阈值为缺省值
	dhcp snooping alarm user-bind threshold *threshold* 例如：[Huawei-Ethernet2/0/0] **dhcp snooping alarm user-bind threshold** 10	（可多选）在接口视图下配置**与绑定表不匹配而被丢弃的 DHCP 报文数**的告警阈值，取值范围是 1～1 000 的整数 缺省情况下，接口下 DHCP Snooping 丢弃报文数量的告警阈值为在系统视图下使用 **dhcp snooping alarm threshold** *threshold* 命令配置的值，可用 **undo dhcp snooping alarm threshold** 命令恢复对应接口的告警阈值为缺省值 【说明】如果在系统视图、接口视图下同时进行了配置，则接口下 DHCP Snooping 丢弃报文数量的告警阈值以两者最小值为准

5.10.3　配置防止 DHCP 服务器拒绝服务攻击

为了抑制 DHCP 用户恶意申请 IP 地址，可配置接口允许学习的 DHCP Snooping 绑定表项的最大个数，当用户数达到该值时，则任何用户将无法通过此接口成功申请到 IP 地址。为了防止攻击者不断改变 DHCP Request 报文中的 CHADDR 字段进行攻击，可使能检测 DHCP Request 报文帧头 MAC 地址与 DHCP 数据区中 CHADDR 字段是否相同的功能，相同则转发报文，否则丢弃。

防止 DHCP 服务器拒绝服务攻击的配置步骤如表 5-18 所示。

表 5-18 **防止 DHCP 服务器拒绝服务攻击的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
配置最大接入用户数（**可在 VLAN 视图或者接口视图下配置**）		
2	**dhcp snooping user-alarm percentage** *percent-lower-value percent-upper-value* 例如：[Huawei] **dhcp snooping user-alarm percentage** 30 80	配置 DHCP Snooping 绑定表的告警阈值百分比。**这条命令只有 V2R5 的版本才有**。当实际学习到的 DHCP Snooping 绑定表项数占下面将要配置的设备允许学习的最大表 项数的比例等于或高于上限告警阈值百分比时，设备将会发出告警。之后，如果该比例又等于或小于下限告警阈值百分比，设备会再次发出告警。命令中的参数说明如下。 ● *percent-lower-value*：指定 DHCP Snooping 绑定表的下限告警阈值百分比，取值范围是 1～100 ● *percent-upper-value*：指定 DHCP Snooping 绑定表的上限告警阈值百分比，取值范围是 1～100，但一定要高于 *percent-lower-value* 参数值 缺省情况下，DHCP Snooping 绑定表的下限告警阈值百分比为 50，上限告警阈值百分比为 100，可用 **undo dhcp snooping user-alarm percentage** 命令取消配置的 DHCP Snooping 绑定表的告警阈值百分比
3	**vlan** *vlan-id* 例如：[Huawei] **vlan** 10	（二选一）键入要配置最大接入用户数的 VLAN，进入 VLAN 视图
	interface *interface-type interface-number* 例如：[Huawei] **interface** ethernet 2/0/0	（二选一）键入要配置最大接入用户数的接口，进入接口视图
4	**dhcp snooping max-user-number** *max-number* 例 如 ： [Huawei-vlan10]**dhcp snooping max-user-number** 100 或[Huawei-Ethernet2/0/0]**dhcp snooping max-user-number** 20	配置接口允许学习的 DHCP Snooping 绑定表项的最大个数，取值范围为 1～1 024 的整数 如果是在 VLAN 视图下配置的，则 VLAN 内所有的接口接入的总用户最大数为该命令所配置的值；如果是在接口视图配置的，则仅指对应接口下的用户最大数 缺省情况下，单个接口允许学习的 DHCP Snooping 绑定表项的最大个数不同版本有所不同，V2R5 版本为 1 024，可用 **undo dhcp snooping max-user-number** 命令恢复接口允许学习的 DHCP Snooping 绑定表项的最大个数为缺省值
使能对报文的 CHADDR 字段进行检查功能（**可在 VLAN 视图或接口视图下配置**）		
5	**dhcp snooping check mac-address enable** 例如：[Huawei-vlan10]**dhcp snooping check mac-address enable** 或[Huawei-Ethernet2/0/0]**dhcp snooping check mac-address enable**	使能检测 DHCP Request 报文帧头 MAC 地址与 DHCP 数据区中 CHADDR 字段是否一致功能 【说明】正常情况下 DHCP Request 报文中 CHADDR 字段与发送该报文的客户端 MAC 地址是相同的，同时 DHCP Server 通常仅根据 CHADDR 字段来确认客户端的 MAC 地址。如果攻击者通过不断改变 DHCP Request 报文中的 CHADDR 字段向 DHCP Server 申请 IP 地址，会导致 DHCP Server 上的地址池被耗尽，从而无法为其他正常用户提供 IP 地址

（续表）

步骤	命令	说明
5	**dhcp snooping check mac-address enable** 例如：[Huawei-vlan10]**dhcp snooping check mac-address enable** 或[Huawei-Ethernet2/0/0]**dhcp snooping check mac-address enable**	在 VLAN 视图下执行此命令，则对 DHCP Snooping 设备上所有接口接收到的属于该 VLAN 的 DHCP 报文都将检测 DHCP Request 报文帧头 MAC 与 DHCP 数据区中 CHADDR 字段是否一致 缺省情况下，未使能检测 DHCP Request 报文帧头 MAC 与 DHCP 数据区中 CHADDR 字段是否一致功能，可用 **undo dhcp snooping check mac-address enable** 命令去使能该功能
6	按照表 5-17 第 5 步的方法**在系统视图或接口视图下配置** DHCP Snooping 丢弃报文数量的告警阈值	

5.10.4 DHCP Snooping 的攻击防范功能配置示例

本示例的基本网络结构如图 5-15 所示，RouterA 与 RouterB 为接入设备，RouterC 为 DHCP 中继。Client1 与 Client2 分别通过 Eth2/0/0 与 Eth2/0/1 接入 RouterA，Client3 通过 Eth2/0/0 接入 RouterB，其中 Client1 与 Client3 通过 DHCP 方式获取 IP 地址，而 Client2 使用静态配置的 IP 地址。网络中存在非法用户的攻击导致合法用户不能正常获取 IP 地址，管理员希望能够防止网络中针对 DHCP 的攻击，为 DHCP 用户提供更优质的服务。

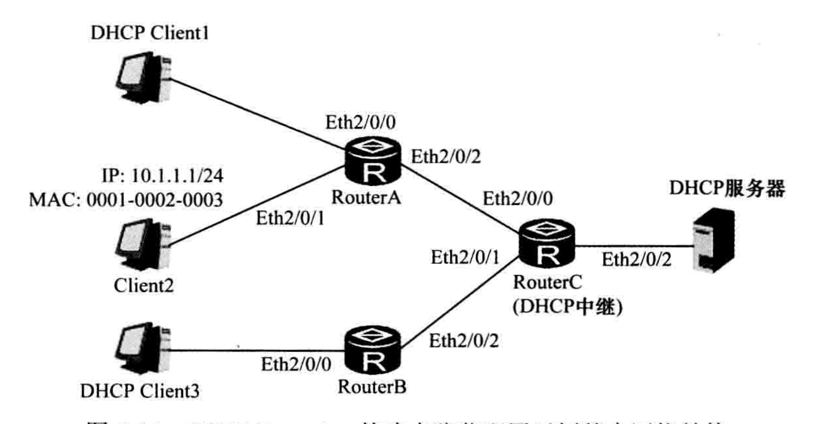


图 5-15　DHCP Snooping 的攻击防范配置示例基本网络结构

1. 基本配置思路分析

本示例的要求比较含糊，因为前面介绍的各种 DHCP 攻击（包括仿冒 DHCP 服务器攻击、仿冒 DHCP 报文攻击和 DHCP 服务器拒绝服务攻击）都可能最终导致合法用户不能正常从 DHCP 服务器中获取 IP 地址，所以本示例需要全面配置防止这些攻击的方法。具体可以在 RouterC 上进行如下配置。

① 使能 DHCP Snooping 功能，这是基本配置，只有使能了它，其他防止 DHCP 攻击功能才能进行配置。

② 配置接口的信任状态，防止仿冒 DHCP 服务器攻击，以保证客户端从合法的服务器获取 IP 地址。

③ 使能 ARP 与 DHCP Snooping 的联动功能，防止仿冒合法用户进行欺骗攻击，保证 DHCP 用户在异常下线时实时更新绑定表。

④ 使能对 DHCP 报文进行绑定表匹配检查的功能，防止仿冒 DHCP 报文攻击。

⑤ 配置允许接入的最大用户数以及使能检测 DHCP Request 报文帧头 MAC 与 DHCP 数据区中 CHADDR 字段是否一致功能，防止 DHCP 服务器拒绝服务攻击。

2. 具体配置步骤

① 使能 DHCP Snooping 功能，包括全局使能和在接口上使能。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] dhcp enable
[RouterC] dhcp snooping enable
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping enable
[RouterC-Ethernet2/0/0] quit
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] dhcp snooping enable
[RouterC-Ethernet2/0/1] quit
```

② 配置接口的信任状态：将连接 DHCP 服务器的接口状态配置为“信任”状态，其他接口保持为缺省的“非信任”状态。

```
[RouterC] interface ethernet 2/0/2
[RouterC-Ethernet2/0/2] dhcp snooping trusted
[RouterC-Ethernet2/0/2] quit
```

③ 使能 ARP 与 DHCP Snooping 的联动功能，防止仿冒合法用户进行欺骗攻击。

```
[RouterC] arp dhcp-snooping-detect enable
```

④ 在用户侧接口使能对 DHCP 报文进行绑定表匹配检查功能，防止仿冒 DHCP 报文攻击。

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping check user-bind enable
[RouterC-Ethernet2/0/0] quit
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] dhcp snooping check user-bind enable
[RouterC-Ethernet2/0/1] quit
```

⑤ 在用户侧接口使能检测 DHCP Request 报文中 GIADDR 字段是否非零的功能。

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping check dhcp-giaddr enable
[RouterC-Ethernet2/0/0] quit
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] dhcp snooping check dhcp-giaddr enable
[RouterC-Ethernet2/0/1] quit
```

⑥ 在用户侧接口配置允许接入的最大用户数（如 20），并使能对 CHADDR 字段检查功能。

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping max-user-number 20
[RouterC-Ethernet2/0/0] dhcp snooping check mac-address enable
[RouterC-Ethernet2/0/0] quit
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] dhcp snooping max-user-number 20
[RouterC-Ethernet2/0/1] dhcp snooping check mac-address enable
[RouterC-Ethernet2/0/1] quit
```

⑦ 在用户侧接口配置丢弃报文告警阈值和报文限速告警功能。

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping alarm mac-address enable
[RouterC-Ethernet2/0/0] dhcp snooping alarm user-bind enable
[RouterC-Ethernet2/0/0] dhcp snooping alarm untrust-reply enable
[RouterC-Ethernet2/0/0] dhcp snooping alarm mac-address threshold 120
[RouterC-Ethernet2/0/0] dhcp snooping alarm user-bind threshold 120
[RouterC-Ethernet2/0/0] dhcp snooping alarm untrust-reply threshold 120
[RouterC-Ethernet2/0/0] quit
[RouterC] interface ethernet 2/0/1
[RouterC-Ethernet2/0/1] dhcp snooping alarm mac-address enable
[RouterC-Ethernet2/0/1] dhcp snooping alarm user-bind enable
[RouterC-Ethernet2/0/1] dhcp snooping alarm untrust-reply enable
[RouterC-Ethernet2/0/1] dhcp snooping alarm mac-address threshold 120
[RouterC-Ethernet2/0/1] dhcp snooping alarm user-bind threshold 120
[RouterC-Ethernet2/0/1] dhcp snooping alarm untrust-reply threshold 120
[RouterC-Ethernet2/0/1] quit
```

配置好后，可以执行 **display dhcp snooping configuration** 命令查看 DHCP Snooping 的配置信息，验证配置结果，具体略。还可执行 **display dhcp snooping interface** 命令查看接口下的 DHCP Snooping 运行信息，具体略。

5.11　配置在 DHCP 报文中添加 Option82 字段

为使 DHCP 服务器能够获取到 DHCP 用户的精确物理位置信息，可在 DHCP 报文中添加 Option82 字段，Option82 选项记录了 DHCP 客户端的位置信息。设备通过在 DHCP 请求报文中添加 Option82 选项，可将 DHCP 客户端的位置信息发送给 DHCP 服务器，从而使得 DHCP 服务器能够根据 Option82 选项的内容为 DHCP 客户端分配合适的 IP 地址和其他配置信息，并可以实现对客户端的安全控制。**不过，本部分内容因为涉及各种格式，比较复杂，通常不用配置。**

DHCP Option82 必须配置在设备的用户侧，否则设备向 DHCP 服务器发出的 DHCP 报文不会携带 Option82 选项内容。具体配置步骤如表 5-19 所示。

表 5-19　　在 DHCP 报文中添加 Option82 字段的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
使能在 DHCP 报文中添加 Option82 选项功能（**可在 VLAN 视图或者接口视图下配置**）		
2	**vlan** *vlan-id* 例如：[Huawei] **vlan** 10	（二选一）键入要使能在 DHCP 报文中添加 Option82 选项功能的 VLAN，进入 VLAN 视图
	interface *interface-type interface-number* 例如：[Huawei] **interface** ethernet 2/0/0	（二选一）键入要使能在 DHCP 报文中添加 Option82 选项功能的接口，进入接口视图

（续表）

步骤	命令	说明
3	**dhcp option82** { **insert** | **rebuild** } **enable** 例如：[Huawei-vlan10] **dhcp option82 insert enable** 或 [Huawei-Ethernet2/0/0]**dhcp option82 insert enable**	使能在 DHCP 报文中添加 Option82 选项功能。命令中的选项说明如下 • **insert**：二选一选项，指定使能在 DHCP 报文中插入 Option82 选项功能，即当设备收到 DHCP 请求报文时，若该报文中没有 Option82 选项，则插入 Option82 选项；若该报文中含有 Option82 选项，则判断 Option82 选项中是否包含 remote-id，如果包含，则保持 Option82 选项不变，如果不包含，则插入 remote-id • **rebuild**：二选一选项，指定使能在 DHCP 报文中强制插入 Option82 选项功能，即当设备收到 DHCP 请求报文时，若该报文中没有 Option82 选项，则插入 Option82 选项；若该报文中含有 Option82 选项，则删除该 Option82 选项并插入管理员自己在设备上配置的 Option82 选项 对于 Insert 和 Rebuild 两种方式，当设备接收到 DHCP 服务器的响应报文时，处理方式一致：若该报文中含有 Option82 选项，则删除之，并转发给 DHCP client；若报文中不含有 Option82 选项，则直接转发
配置 DHCP Snooping 丢弃报文数量的告警阈值（**可在系统视图或接口视图下配置**）		
4	**dhcp option82 [circuit-id | remote-id] format { default | common | extend | user-defined** *text* **}** 例如：[Huawei] **dhcp option82 circuit-id format user-defined** "%portname:%svlan.%cvlan %sysname"	（可选）**在系统视图下**配置在 DHCP 报文中添加的 Option82 选项的格式。命令中的参数和选项说明如下。 • **circuit-id**：二选一选项，指定配置 Option82 的 circuit-id（CID）子选项。若不选择该子选项，则其格式为缺省格式 default • **remote-id**：二选一选项，指定配置 Option82 的 remote-id（RID）子选项。若不选择该子选项，则其格式为缺省格式 **default** • **default**：多选一选项，指定 Option82 选项为默认格式，即 CID 的格式为“接口名:svlan.cvlan 主机名/0/0/0/0/0”，采用 ASCII 封装；RID 的格式为“设备 MAC 地址”，采用十六进制封装 • **common**：多选一选项，指定 Option82 选项为通用格式，即 CID 的格式为“{eth|trunk}槽位号/子卡号/端口号:svlan.cvlan 主机名/0/0/0/0/0”，采用 ASCII 封装；RID 的格式为“设备 MAC 地址”，也采用 ASCII 封装 • **extend**：多选一选项，指定 Option82 选项为扩展格式，即 CID 的格式为“circuit-id type(0)+ length(4)+SVLAN (2byte)+slot(5bit)+subslot(3bit) +port(1byte)”，十六进制封装；RID 的格式为“remote-id type(0)+length(6)+mac (6byte)”，采用十六进制封装 • **user-defined** *text*：多选一参数，指定 Option82 选项格式为用户自定义格式。**具体内容比较多，不作介绍，请参考产品手册** 缺省情况下，DHCP 报文中添加的 Option82 选项的格式为 **default**，可用 **undo dhcp option82 [circuit-id | remote-id] format** 命令恢复在 DHCP 报文中添加的 Option82 选项的格式为缺省格式

（续表）

步骤	命令	说明
4	**dhcp option82** [**vlan** *vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** **text** } 例如：[Huawei-Ethernet2/0/0] **dhcp option82 vlan** 10 **format extend**	（可选）**在接口视图下**配置在 DHCP 报文中添加的 Option82 选项的格式。与上一命令相比，多了一个 **vlan** *vlan-id* 可选参数，用来指定所设置的 Options 格式所作用的 VLAN 的编号。如果指定本参数，则仅会配置属于该 VLAN 的 DHCP 报文中的 Option82 选项的格式；如果不指定本参数，则会配置接口下所有的 DHCP 报文中的 Option82 选项的格式。其他参数说明参见在系统视图下执行本命令介绍 缺省情况下，DHCP 报文中添加的 Option82 选项的格式为 **default**，可用 **undo dhcp option82** [**vlan** *vlan-id*] [**circuit-id** | **remote-id**] **format** 命令恢复在 DHCP 报文中添加的 Option82 选项的格式为缺省格式

5.12　DNS 服务配置与管理

DNS 是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换服务。AR G3 系列路由器支持作为 DNS 客户端、DNS 代理/中继（Proxy/Relay）和 DDNS 客户端（**不能配置作为 DNS 服务器**）。因篇幅原因，DNS、DNS 代理/中继（Proxy/Relay）和 DDNS 的工作原理在此不作介绍，请参考相关专业图书，如《深入理解计算机网络》。

5.12.1　配置作为 DNS 客户端

当把 AR G3 系列路由器配置作为 DNS 客户端使用时，支持静态域名解析和动态域名解析。静态域名解析即手动建立域名和 IP 地址之间的对应关系。在设备上配置静态域名表项后，当 DNS 客户端需要域名所对应的 IP 地址时，会查询静态域名解析表，获得域名所对应的 IP 地址。

动态域名解析有专用的 DNS 服务器，负责接收 DNS 客户端提出的域名解析请求。DNS 服务器首先在本机数据库内部解析，如果判断不属于本域范围之内，就将请求交给上一级的 DNS 服务器，直到完成解析，解析的结果为获得域名对应的 IP 地址或者该域名对应的 IP 地址不存在，DNS 服务器将最终解析的结果反馈给 DNS 客户端。

DNS 客户端的静态域名解析和动态域名解析（**二者选其一**）的配置方法如表 5-20 所示。

表 5-20　DNS 客户端的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
配置静态 DNS 客户端		
2	**ip host** *host-name ip-address* 例如：[Huawei] **ip host** www.huawei.com 10.10.10.4	配置静态 DNS 表项。命令中的参数说明如下 *host-name*：指定要解析的域名，1～24 字符，**不支持空格，区分大小写**

（续表）

步骤	命令	说明
2	**ip host** *host-name ip-address* 例如：[Huawei] **ip host** www.huawei.com 10.10.10.4	*ip-address*：指定以上域所对应的 IP 地址 缺省情况下，未配置静态 DNS 表项 【注意】每个主机名只能对应一个 IP 地址，当对同一主机名进行多次配置时，最后配置的 IP 地址有效。如果有多个主机名需要解析，则需要重复本步骤
配置动态 DNS 客户端		
2	**dns resolve** 例如：[Huawei] **dns resolve**	使能动态域名解析功能。如果用户希望使用动态域名解析功能，通过 DNS 服务器来获取域名对应的 IP 地址，则需要在设备上通过本命令来使能设备的动态域名解析功能 缺省情况下，动态域名解析功能处于未使能状态，可用 **undo dns resolve** 命令去使能动态域名解析功能
3	**dns server** *ip-address* 例如：[Huawei] **dns server** 10.10.1.1	配置 DNS 客户端访问的 DNS 服务器的 IP 地址。系统支持最多可以配置 6 个 DNS 服务器的 IP 地址，如果需要配置多个时则要重复配置本命令 缺省情况下，没有配置 DNS 服务器的 IP 地址，可用 **undo dns server** [*ip-address*]命令删除指定的或者所有配置的 DNS 服务器 IP 地址
4	**dns server source-ip** *ip-address* 例如：[Huawei]**dns server source-ip** 172.16.1.10	（可选）指定本端设备作为 DNS 客户端，进行 DNS 报文交互时的源 IP 地址，可以是自己设备的地址，也可以不是，但一定要使 DNS 服务器可达 缺省情况下，未配置 DNS 报文交互时的源 IP 地址，可用 **undo dns server source-ip** 命令删除设备进行 DNS 报文交互时的源 IP 地址
5	**dns-server-select-algorithm** { **fixed** | **auto** } 例如：[Huawei]**dns-server-select-algorithm auto**	（可选）配置设备选择目的 DNS 服务器算法。命令中的选项说明如下 ● **fixed**：二选一选项，配置目的 DNS 服务器选择算法为 fixed（固定）顺序算法。此时，设备每次发送 DNS 查询请求时，首先都会向配置的第一个 DNS 服务器发送 DNS 查询请求，如果在规定时间内没有收到响应，则重新发送 DNS 查询请求，如果重新发送多次 DNS 查询请求后，设备仍然没有得到 DNS 服务器回应，则向下一个 DNS 服务器查询请求，依次进行，直到得到响应或者依次查询完所有配置的 DNS 服务器为止。这样就保证主服务器发生故障又恢复正常后，设备优先选择的 DNS 服务器仍为主服务器 ● **auto**：二选一选项，配置目的 DNS 服务器选择算法为 auto（自动）顺序算法。此时，当主 DNS 服务器出现故障后，设备会将目的 DNS 服务器切换至备用 DNS 服务器，但是当主 DNS 服务器恢复正常后，设备无法从备用 DNS 服务器切换到主 DNS 服务器 缺省情况下，系统选择 DNS 服务器的算法为 auto 顺序算法

（续表）

步骤	命令	说明
6	**dns forward retry-number** *number* 例如：[Huawei]**dns forward retry-number** 3	（可选）配置设备向目的DNS服务器发送查询请求的重传次数，取值范围为0～15的整数 【说明】DNS查询请求的重传次数配置和下一步将要介绍的重传超时时间配置结合才能确定设备的查询超时时间。 当选择目的DNS服务器算法为auto顺序算法时，DNS设备超时时间为=（重传次数+1）×重传超时时间；当选择目的DNS服务器算法为fixed顺序算法时，DNS设备超时时间为=（重传次数+1）×重传超时时间×DNS服务器个数 缺省情况下，系统向目的DNS服务器发送查询请求的重传次数为2次，可用 **undo dns forward retry-number** 命令恢复向目的DNS服务器发送查询请求的重传次数为缺省值
7	**dns forward retry-timeout** *time* 例如：[Huawei]**dns forward retry-timeout** 10	（可选）配置设备向目的DNS服务器发送查询请求的超时重传时间，取值范围为（0～15）的整数秒。**本命令只有V2R5的版本才有** 缺省情况下，系统向目的DNS服务器发送查询请求的超时重传时间是3 s，可用 **undo dns forward retry-timeout** 命令恢复向目的DNS服务器发送查询请求的重传超时时间为缺省值
8	**dns domain** *domain-name* 例如：[Huawei] **dns domain** com.cn	（可选）配置域名后缀，1～63个字符，不支持空格，区分大小写，可以设定为包含数字、字母和下划线“_”或“.”的组合。公网中的域名后缀必须是在域名颁发机构注册的，如com、cn、com.cn、org、net等。设置域名后缀是为了便于在访问对应主机时可不用输入其域名，只需输入其前面NetBIOS名部分即可 DNS客户端最多支持10个域名后缀，用户如果想要配置多个域名后缀，可重复配置本命令 缺省情况下，DNS客户端上未配置域名后缀，可用 **undo dns domain** [*domain-name*]命令删除DNS客户端上配置的指定或全部域名后缀

5.12.2　配置DNS Proxy/Relay

AR G3系列路由器可以配置作为DNS Proxy/Relay（代理/中继）使用，转发DNS请求和应答报文，实现DNS客户端的域名解析功能，主要包括如下两项配置任务。在配置DNS Proxy/Relay之前，需要配置好对应的DNS服务器以及与DNS客户端和DNS服务器之间的路由。

说明　DNS Relay和DNS Proxy功能相同，区别在于DNS Proxy接收到DNS客户端的DNS查询报文后会查找本地缓存，有时查询的效率更高；而DNS Relay不会查询本地缓存，而是直接转发给DNS服务器进行解析，从而节省了DNS Relay上的DNS缓存开销，

但查询效率往往较低。

（1）配置目的 DNS 服务器

本项配置任务首先要全局使能 DNS Proxy/Relay 功能，然后配置 DNS Proxy/Relay 要访问的目的 DNS 服务器及相关的参数属性。

在设备上使能 DNS Proxy 或者 DNS Relay 功能后，可用于在 DNS Client 和 DNS Server 之间转发 DNS 请求和应答报文。局域网内的 DNS 客户端把 DNS Proxy 或者 DNS Relay 当作 DNS 服务器，将 DNS 请求报文发送给 DNS Proxy 或 DNS Relay。DNS Proxy 或 DNS Relay 将该请求报文转发到真正的 DNS 服务器，并将 DNS 服务器的应答报文返回给 DNS 客户端，从而实现域名解析。当配置设备作为 DNS Proxy 或 DNS Relay 后，可为企业网用户提供 DNS 服务器功能，用户无需直接和 DNS 服务器进行交互，简化了路由部署，同时提高了 DNS 服务器性能和安全性。

（2）（可选）配置 DNS Spoofing 功能

当设备使能 DNS Proxy/Relay 功能后，如果设备上没有配置 DNS 服务器地址或不存在到达 DNS 服务器的路由，则设备不会转发 DNS 服务器的域名解析请求，也不会应答该请求。如果此时设备上同时使能了 DNS Spoofing 功能，则会利用配置的 IP 地址作为域名解析结果，欺骗性地应答域名解析请求。

【经验之谈】其实 DNS Spoofing 功能非常常见，如我们通常会把宽带路由器当成 DNS 服务器使用，其实宽带路由器本身不具备 DNS 服务器功能，所使用的就是 DNS Spoofing 功能。但如果在路由器上没有使能 DNS Spoofing 功能时，路由器接收到主机发送的域名解析请求报文后，如果不存在对应的域名解析表项，则需要向 DNS 服务器发送域名解析请求。但由于此时拨号接口尚未建立连接，路由器上不存在 DNS 服务器地址，Router 不会向 DNS 服务器发送域名解析请求，也不会应答 DNS 客户端的请求，最终导致域名解析失败，且没有流量触发拨号接口建立连接。

如果使能了 DNS Spoofing 功能，即使路由器上不存在 DNS 服务器的 IP 地址或到达 DNS 服务器的路由，路由器也会利用指定的 IP 地址作为域名解析结果，应答 DNS 客户端的域名解析请求。DNS 客户端后续发送的报文可以用来触发拨号接口建立连接。

要让 DNS Spoofing 生效，除了需要使能 DNS Proxy 或者 DNS Relay 外，还需要满足如下条件之一。

① 没有配置 DNS 服务器，或者配置了 DNS 服务器，但是没有使能 DNS 动态解析功能。

② 没有到达 DNS 服务器的路由。

③ 通往 DNS 服务器的出接口上没有可用的源 IP 地址。

当满足以上某一个条件，DNS Proxy 或者 DNS Relay 接收到一个 A 类（主机类）查询时，使用 DNS Spoofing 配置的 IP 地址进行应答。

以上两项 DNS Proxy/Relay 配置任务的具体配置步骤如表 5-21 所示。在“目的 DNS 服务器”配置任务中，总体与 5.2.1 小节表 5-20 中的动态 DNS 解析配置一样，只不过这里多了一个使能 DNS Proxy 或者 DNS Relay 功能的配置。

表 5-21 **DNS Proxy/Relay 的配置步骤**

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
配置目的 DNS 服务器	2	**dns proxy enable** 或 **dns relay enable** 例如：[Huawei] **dns proxy enable** 或[Huawei] **dns relay enable**	使能 DNS Proxy 或 DNS Relay 功能 缺省情况下，系统未使能 DNS Proxy 或 DNS Relay 功能，可分别用 **undo dns proxy enable、undo dns relay enable** 命令去使能 DNS Proxy 或 DNS Relay 功能
	3	**dns resolve** 例如：[Huawei] **dns resolve**	使能动态域名解析功能。其他说明参见 5.12.1 小节表 5-20 中动态 NDS 解析配置中的第 2 步
	4	**dns server** *ip-address* 例如：[Huawei] **dns server** 10.10.1.1	配置 DNS Proxy/Relay 访问的 DNS 服务器。其他说明参见 5.12.1 小节表 5-20 中动态 NDS 解析配置中的第 3 步
	5	**dns server source-ip** *ip-address* 例如：[Huawei]**dns server source-ip** 172.16.1.10	（可选）指定与 DNS 服务器进行 DNS 报文交互时的源 IP 地址。其他说明参见 5.12.1 小节表 5-20 中动态 NDS 解析配置中的第 4 步
	6	**dns-server-select-algorithm** { **fixed** | **auto** } 例如：[Huawei]**dns-server-select-algorithm auto**	（可选）配置 DNS Proxy/Relay 选择目的 DNS 服务器算法。其他说明参见 5.12.1 小节表 5-20 中动态 NDS 解析配置中的第 5 步
	7	**dns forward retry-number** *number* 例如：[Huawei]**dns forward retry-number** 3	（可选）配置 DNS Proxy/Relay 向目的 DNS 服务器发送查询请求的重传次数。**这条命令只有 V2R5 的版本才有**。其他说明参见 5.12.1 小节表 5-20 中动态 NDS 解析配置中的第 6 步
	8	**dns forward retry-timeout** *time* 例如：[Huawei]**dns forward retry-timeout** 10	（可选）配置 DNS Proxy/Relay 向目的 DNS 服务器发送查询请求的超时重传时间。其他说明参见 5.12.1 小节表 5-20 中动态 NDS 解析配置中的第 7 步
配置 DNS Spoofing 功能	9	**dns spoofing** *ip-address* 例如：[Huawei]**dns spoofing** 192.168.1.1	（可选）使能 DNS Spoofing 功能，并指定应答的 IP 地址 缺省情况下，系统未使能 DNS Spoofing 功能，可用 **undo dns spoofing** 命令去使能 DNS Spoofing 功能

5.12.3 配置 DDNS 客户端

DNS 仅提供了域名和 IP 地址之间的静态对应关系，当节点的 IP 地址发生变化时，DNS 无法动态地更新域名和 IP 地址的对应关系。此时，如果仍然使用域名访问该节点，则通过域名解析得到的 IP 地址是错误的，从而导致访问失败。动态域名系统 DDNS 可用来动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的 IP 地址。

DDNS 也采用的客户端/服务器工作模式，具体工作原理如下。

① DDNS 客户端：DDNS 客户端就是向 DDNS 发出动态域名解析的设备，如各种

需要进行域名解析的应用服务器。为保证在这些需要进行域名解析的应用服务器 IP 地址变化时，其他用户仍然可以通过域名访问这些应用服务器，需要将这些应用服务器配置为 DDNS 客户端，向 DDNS 服务器发送更新域名和 IP 地址对应关系的 DDNS 更新请求。

② DDNS 服务器：DDNS 服务器负责通知 DNS 服务器动态更新域名和 IP 地址之间的对应关系。在接收到 DDNS 客户端的更新请求后，DDNS 服务器通知 DNS 服务器重新建立 DDNS 客户端的域名和 IP 地址之间的对应关系，从而保证即使 DDNS 客户端的 IP 地址改变，Internet 用户仍然可以通过同样的域名访问 DDNS 客户端。

DDNS 的更新过程没有统一的标准，不同的 DDNS 服务器请求更新的过程各不相同。AR G3 系列路由器所支持的 DDNS 服务提供商主要有 www.3322.org、www.oray.cn、www.dyndns.com 等。在配置 DNS 客户端之前，需要在对应的 DDNS 服务器网站上进行用户注册，并配置好设备与 DDNS 服务器之间的路由。担当 DDNS 客户端的设备端需要配置以下两项任务。

（1）配置 DDNS 策略

通过配置 DDNS 策略，可以指定在接口 IP 地址发生变化后，DDNS 更新请求发送到目的 DDNS 服务器。

（2）绑定 DDNS 策略

通过在接口上应用指定的 DDNS 策略来更新指定的 FQDN（Fully Qualified Domain Name，完全合格域名）与 IP 地址的对应关系，并启动 DDNS 更新。

以上两项 DDNS 客户端配置任务的具体配置步骤如表 5-22 所示。

表 5-22 DDNS 客户端的配置步骤

配置任务	步骤	命令	说明
公共配置	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
配置 DDNS 策略	2	**ddns policy** *policy-name* 例如：[Huawei] **ddns policy** mypolicy	创建 DDNS 策略，并进入 DDNS 策略视图。参数 *policy-name* 用来指定创建的 DDNS 策略名称，1～32 个字符，不支持空格，区分大小写。支持最多配置 10 个 DDNS 策略 缺省情况下，系统未创建 DDNS 策略，可用 **undo ddns policy** *policy-name* 命令删除指定的 DDNS 策略
	3	**url** *request-url* 例如：[Huawei-ddns-policy-mypolicy]**url** http://steven:nevets@members.3322.org/dyndns/update'system=dyndns&hostname=<h>&ip=<a>	指定 DDNS 更新请求的 URL 地址。参数 *request-url* 用来指定请求的 URL 地址，20～256 个字符，不支持空格，区分大小写，包含用户名和密码等信息，且用户名和密码的配置信息以明文显示 使能 DDNS 策略后，需填写 URL 地址，说明此策略与哪个 DDNS 服务提供商相连。设备向不同 DDNS 服务器请求更新的过程各不相同，因此，DDNS 服务器 URL 地址的配置方式也存在差异 • 设备基于 HTTP 与 www.3322.org 通信时，DDNS 更新请求的 URL 地址格式为：http://username:password@members.3322.org/dyndns/update?system=dyndns&hostname=<h>&ip=<a>

（续表）

配置任务	步骤	命令	说明
配置 DDNS 策略	3	**url** *request-url* 例如：[Huawei-ddns-policy-mypolicy]**url** http://steven:nevets@members.3322.org/dyndns/update'system=dyndns&hostname=<h>&ip=<a>	• 设备基于 HTTP 与 www.dyndns.com 通信时，DDNS 更新请求的 URL 地址格式为：http://username:password@update.dyndns.com/nic/update?hostname=<h>&myip=<a> • 设备基于 TCP 与 www.oray.cn 通信时，DDNS 更新请求的 URL 地址格式为：oray://username:password@phddnsdev.oray.net • 设备基于 HTTPS 与西门子类型的 DDNS 服务器通信时，DDNS 更新请求的 URL 地址是自由定义类型，比如:https://194.138.36.67/nic/update?group=med&user=huawei_test&password=12345&myip=192.168.19.2 缺省情况下，设备没有指定 DDNS 更新请求的 URL 地址，可用 **undo url** 命令删除已指定的 DDNS 更新请求的 URL 地址
	4	**ssl-policy** *policy-name* 例如：[Huawei-ddns-policy-mypolicy] **ssl-policy** siemens	在 DDNS 策略下绑定 SSL 策略。参数 *policy-name* 用来指定以上要绑定在 DDNS 策略下的 SSL 策略的名称 只有西门子的 DDNS 服务器通信时才需要绑定 SSL 策略，对于其他两种的 DDNS 策略不需要绑定 SSL 策略 缺省情况下，系统在 DDNS 策略下未绑定 SSL 策略，可用 **undo ssl-policy** 命令删除绑定的 SSL 策略
	5	**interval** *interval-time* 例如：[Huawei-ddns-policy-mypolicy] **interval** 3600	（可选）指定 DDNS 更新启动后，定时发起更新请求的时间间隔，取值范围为（60～31 536 000）的整数秒。使能 DDNS 策略后，通过设置定时刷新时间间隔来触发定时刷新。 【注意】重复执行本命令，配置不同的 DDNS 更新请求的时间间隔时，后面的配置将覆盖先前的配置 不论是否到达定时发起更新请求的时间，只要对应接口的主 IP 地址发生改变或接口的链路状态由 down 变为 up，都会立即发起更新请求。如果修改了定时刷新时间，会立刻触发一次刷新 缺省情况下，定时发起更新请求的时间间隔为 3 600 s，可用 **undo interval** 命令恢复为缺省的时间间隔
绑定 DDNS 策略	6	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要绑定 DDNS 策略的 DDNS 客户端接口，进入接口视图
	7	**ddns apply policy** *policy-name* [**fqdn** *domain-name*] 例如：[Huawei-GigabitEthernet1/0/0]**undo ddns apply policy** mypolicy	在 DDNS 客户端接口上绑定 DDNS 策略。命令中的参数说明如下 • *policy-name*：指定要绑定的以上创建的 DDNS 策略名称。一个接口上最多可以应用 4 个 DDNS 策略 • **fqdn** *domain-name*：可选参数，指定 DDNS 更新的完全合格域名名称。只有当 DDNS 服务器为 www.3322.org 或 www.dyndns.com 时，才支持配置完全合格域名 FQDN

5.12.4 DNS 管理

配置好以上各项 DNS 功能后，可用以下任意视图命令查看相关信息，验证配置结果，也可用以下用户视图命令相关 DNS 统计信息。

① **display dns forward table** [**source-ip** *ip-address*]：查看所有或者指定的源 IP 地址的 DNS 转发的映射表。

② **display dns dynamic-host**：查看动态 DNS 表项信息。

③ **display dns configuration**：查看 DNS 全局配置信息。

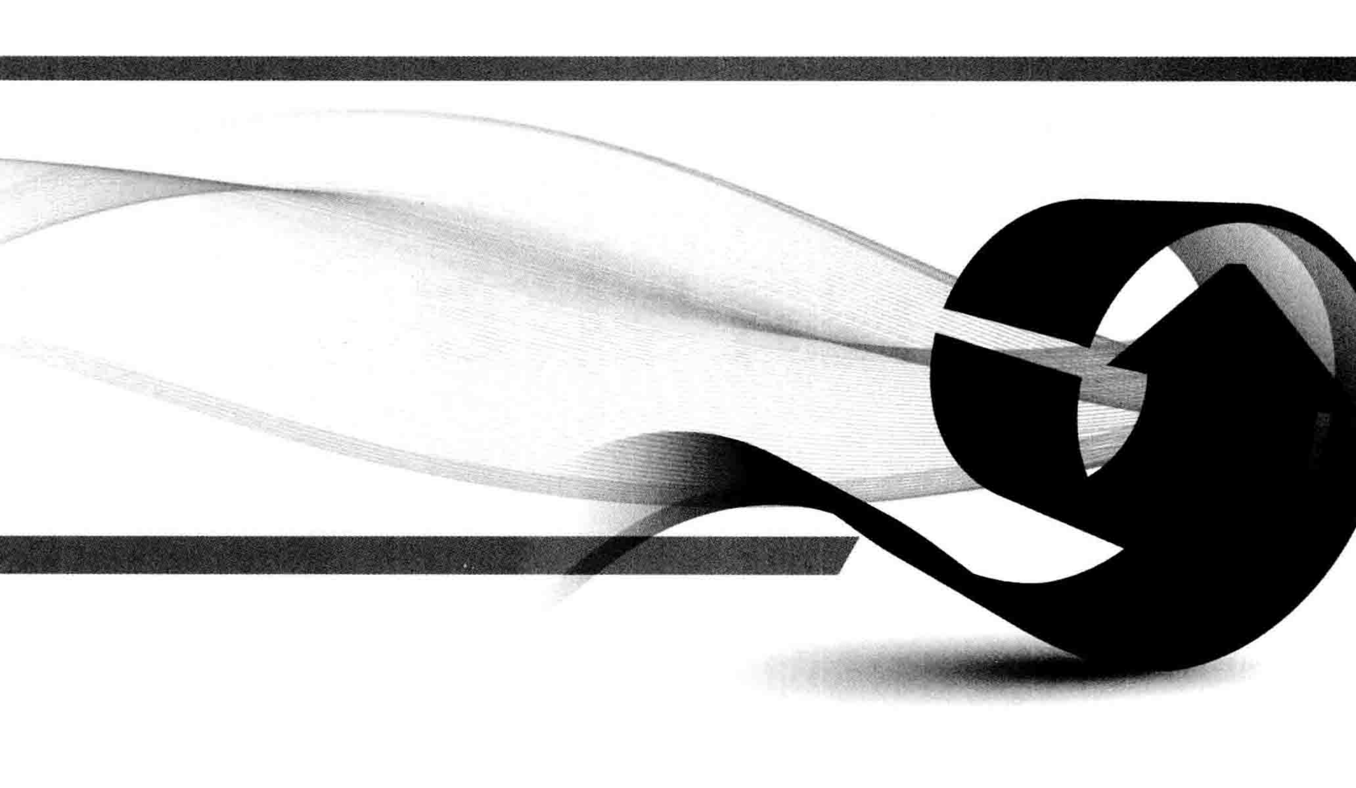
④ **display ddns policy** *policy-name*：查看指定的 DDNS 策略的信息。

⑤ **display ddns interface** *interface-type interface-number*：查看指定接口下的 DDNS 策略信息。

⑥ **reset dns dynamic-host**：清除动态 DNS 表项。

⑦ **reset dns forward table** [**source-ip** *ip-address*]：清除所有或者指定的源 IP 地址的 DNS 转发映射表。

⑧ **reset ddns policy** *policy-name* [**interface** *interface-type interface-num*]：手动刷新指定 DDNS 策略，更新应用此策略的所有 IP 地址和域名间的绑定关系。



第6章
NAT配置与管理



NAT（网络地址转换）是用来在网络间进行IP地址转换的一种技术，可使多个私网（或为“内部网络”）用户通过共享一个或多个公网（或其他私网，也称“外部网络”）IP地址访问Internet公网或者其他私网，也可用于外部网络用户访问内部网络服务器的情形。**本章主要介绍私网与Internet公网之间的IP地址映射。**

其实NAT离我们很近，大多数普通家庭通过宽带路由器接入的Internet就必须要用到它，只不过这是宽带路由器自带的功能，且无需配置，所以很多人并不知道。本章将全面介绍华为AR G3系列路由器中所支持的静态NAT（需要配置固定的NAT地址映射表）、动态NAT（包括Easy IP，需要配置用于动态建立NAT地址映射表的公网地址池）和NAT Server（专用于外网用户访问内网服务器，需要配置内部服务器的私网IP地址、私网端口号与公网IP地址、公网端口号之间的固定映射表）这三种NAT特性，以及像NAT ALG（用对应的私网IP地址替换报文中的公网地址，同时屏蔽报文中的私网地址信息实现在不同网络间穿越）、DNS Mapping（用来实现在内网使用公网域名访问内部服务器）、两次NAT（专用来解决两个地址重叠的网络间的NAT地址转换）、NAT过滤和映射等扩展NAT功能的配置与管理方法。

6.1 NAT 基础

随着 Internet 的发展和网络应用终端的增加，IPv4 地址的日益枯竭早已成为制约全球计算机网络发展的瓶颈。虽然 IPv6 可以从根本上解决 IPv4 地址空间不足的问题，但是 IPv6 的普及还需要一个过程。在此之前，迫切需要一些过渡技术来解决这个问题，NAT（Network Address Translation，网络地址转换）技术就是其中主要的解决手段之一（还有如 VLSM、CIDR 都对此有所帮助）。NAT 可以将来自一个网络的 IP 数据报报头中的 IP 地址（可以是源 IP 地址，或者目的 IP 地址，或者两者同时）转换为另一个网络的 IP 地址，主要用于实现私网用户和公网用户之间的互访。

总体而言，NAT 技术可以带来以下好处。

① 节省公网 IPv4 地址，因为私网内多个用户可以共享一个公网 IP 地址对公网进行访问。

② 在实现地址转换的同时，还隐藏了内网主机的真实 IP 地址，从而防止外部网络对内部主机的攻击，提高了内网的安全性。

③ 控制内网主机访问外网，同时也可以控制外网主机访问内网，解决了内网和外网不能互通的问题。

6.1.1 NAT 主要特性

根据报文中 IP 地址的转换过程以及 NAT 技术的主要应用，在 AR G3 系列路由器中把所支持的 NAT 特性分为三大类：动态 NAT、静态 NAT 和 NAT Server（NAT 服务器）。在实际应用中，它们分别对应配置动态地址转换、配置静态地址转换和配置内部服务器。

1. 动态 NAT

"动态 NAT"，顾名思义，其中的私网 IP 地址与公网 IP 地址之间的转换不是固定的，具有动态性，是通过把需要访问公网的私网 IP 地址动态地与公网 IP 地址建立临时映射关系，并将报文中的私网 IP 地址进行对应的临时替换，待返回报文到达设备时再根据映射表"反向"把公网 IP 地址临时替换回对应的私网 IP 地址，然后转发给主机，实现内网用户和外网的通信。

动态 NAT 的实现方式有 Basic NAT 和 NAPT 两种方式（Easy IP 是 NAPT 的一种特例，主要应用于中小型企业 Internet 接入时的 NAT 地址转换）。Basic NAT 是一种"一对一"的动态地址转换，即一个私网 IP 地址与一个公网 IP 地址进行映射；而 NAPT 则通过引入"端口"变量，是一种"多对一"的动态地址转换，即多个私网 IP 地址可以与同一个公网 IP 地址进行映射（**但所映射的公网端口必须不同**）。目前使用最多的是 NAPT 方式，因为它能提供一对多的映射功能。有关 Basic NAT（基本 NAT）、NAPT（Network Address Port Translation，网络地址端口转换）和 Easy IP 这三种 NAT 的详细实现原理将在本章后面具体介绍。

2. 静态 NAT

动态 NAT 在转换地址时做不到在不同时间固定地使用同一个公网 IP 地址、端口号

替换同一个私网 IP 地址、端口号，因为在动态 NAT 中，具体用哪个公网 IP 地址、端口来与私网 IP 地址、端口进行映射，纯粹是从地址池和端口表中随机选取空闲的地址和端口号。这虽然可以提高公网 IP 地址的利用率（因为所建立的映射是临时的，当用户断开 NAT 应用时将释放所建立的映射），但同时无法让一些内网重要主机固定使用同一个公网 IP 地址访问外网。

静态 NAT 可以建立固定的一对一的公网 IP 地址和私网 IP 地址的映射，特定的私网 IP 地址只会被特定的公网 IP 地址替换，相反亦然。这样，就保证了重要主机使用固定的公网 IP 地址访问外网。但在实际应用中，这种情形并不多见，因为采用固定公网 IP 地址的通常是内部网络服务器，而这时通常是采用下面将要介绍的 NAT Server，主要用于外网用户对内部服务器的访问。

3. NAT Server

前面说到的静态 NAT 和动态 NAT 讲的都是由内网向外网发起访问的情形，这时通过 NAT 一方面可以实现多个内网用户共用一个或者多个公网 IP 地址访问外网，同时又因为私网 IP 地址都经过了转换，所以具有“屏蔽”内部主机 IP 地址的作用。

有时内网需要向外网提供服务，架设于内网的各种服务器（如 Web 服务器、FTP 服务器、邮件服务器等）要向外网用户提供服务。这种情况下需要内网的服务器不能被“屏蔽”，外网用户需要可以随时访问内网服务器。**这是一种由外网发起向内网访问的 NAT 转换情形。**

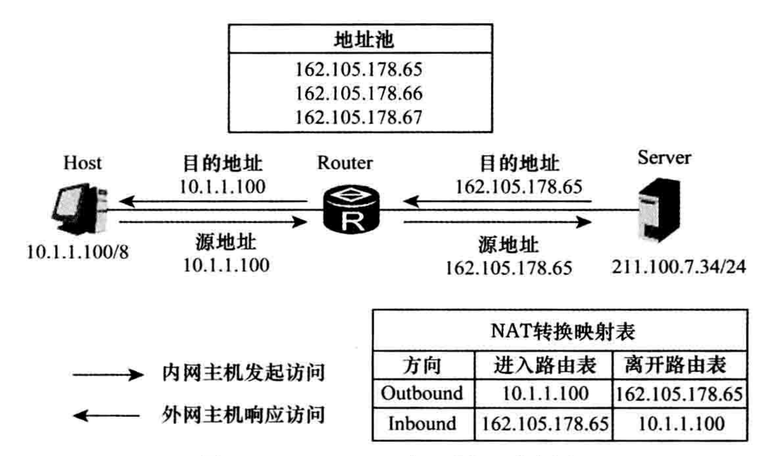
NAT Server 可以很好地解决这个问题。当外网用户访问内网服务器时，它通过事先配置好的服务器的“公网 IP 地址:端口号”与服务器的“私网 IP 地址:端口号”间的固定映射关系，即将服务器的“公网 IP 地址:端口号”根据映射关系替换成对应的“私网 IP 地址:端口号”，以实现外网用户对位于内网的服务器的访问。**从私网 IP 地址与公网 IP 地址的映射关系看，它也是一种静态映射关系。**

6.1.2　Basic NAT 实现原理

Basic NAT 方式属于一对一的地址转换，但要注意它不是静态的一对一转换，而是动态的。

在这种转换方式下，在内网用户向公网发起连起请求时，请求报文中的私网 IP 地址就会通过事先准备好的公网 IP 地址池动态地建立私网 IP 地址与公网 IP 地址的 NAT 映射表项，并利用所映射的公网 IP 地址将报文中的源 IP 地址（也就是内网用户主机的私网 IP 地址）进行替换（但只转换 IP 地址，而不处理 TCP/UDP 协议的端口号，且一个公网 IP 地址不能同时被多个私网 IP 地址映射），然后送达给外网的目的主机。而当外网主机收到请求报文后进行响应时，响应报文到达 NAT 设备后，又将依据前面请求报文所建立的私网 IP 地址与公网 IP 地址的映射关系反向将报文中的目的 IP 地址（为内部主机私网 IP 地址映射后的公网 IP 地址）替换成对应的私网 IP 地址，然后送达给内部源主机。

图 6-1 所示为 Basic NAT 的基本原理，实现过程如下（**需先要在 Router 上创建公网地址池**）。



NAT转换映射表		
方向	进入路由表	离开路由表
Outbound	10.1.1.100	162.105.178.65
Inbound	162.105.178.65	10.1.1.100

图 6-1　Basic NAT 实现原理示意图

① 当内网侧 Host（主机）要访问公网侧 Server（服务器）时，向 Router 发送请求报文（即 Outbound 方向），此时报文中的源 IP 地址为 Host 自己的 10.1.1.100，目的 IP 地址为 Server 的 IP 地址 211.100.7.34。

② Router 在收到来自 Host 的请求报文后，会从事先配置好的公网地址池中选取一个空闲的公网 IP 地址，建立与内网侧报文源 IP 地址间的 NAT 转换映射表项，包括正（Outbound）、反（Inbound）两个方向，然后依据查找正向 NAT 表项的结果将报文中的源 IP 地址转换成对应的公网 IP 地址后向公网侧发送。此时发送的报文的源 IP 地址已是转换后的公网 IP 地址 162.105.178.65（**不再是原来的 Host IP 地址 10.1.1.100**），目的 IP 地址不变，仍为 Server 的 IP 地址 211.100.7.34。

③ 当 Server 收到请求报文后，需要向 Router 发送响应报文（即 Inbound 方向），此时只须将收到的请求报文中的源 IP 地址和目的 IP 地址对调即可，即报文的源 IP 地址就是 Server 自己的 IP 地址 211.100.7.34，目的 IP 地址是 Host 私网 IP 地址转换后的公网 IP 地址 162.105.178.65。

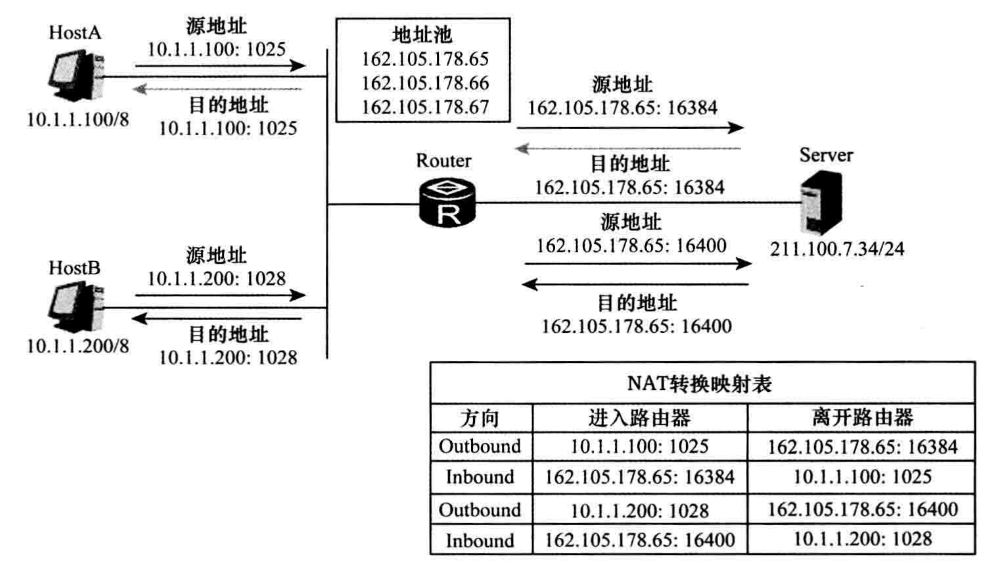
④ 当 Router 收到来自公网侧 Server 发送的响应报文后，会根据报文中的目的 IP 地址查找反向 NAT 映射表项，并根据查找结果将报文中的目的 IP 地址转换成 Host 主机对应的私网 IP 地址（源地址不变）后向私网侧发送，即此时报文中的源 IP 地址仍是 Server 的 IP 地址 211.100.7.34，目的 IP 地址已转换成了 Host 的私网 IP 地址 10.1.1.100。

【经验之谈】从以上 Basic NAT 实现原理分析可以看出，Basic NAT 中的**请求报文转换的仅是其中的源 IP 地址**（目的 IP 地址不变），**即仅需关心源 IP 地址；而响应报文转换的仅是其中的目的 IP 地址**（源 IP 地址不变），**即仅需关心目的 IP 地址**。两个方向所转换的 IP 地址是相反的。

6.1.3 NAPT 实现原理

由于 Basic NAT 这种一对一的转换方式并未实现公网地址的复用，不能有效解决 IP 地址短缺的问题，因此在实际应用中并不常见。而这里要介绍的 NAPT 可以实现并发的地址转换，允许多个内部地址映射到同一个公有地址上，因此也可以称为“多对一地址转换”或地址复用。

NAPT 使用“IP 地址+端口号”的形式进行转换，相当于增加了一个变量，最终可以使多个私网用户共用一个公网 IP 地址访问外网。图 6-2 所示为 NAPT 的实现原理，具体过程如下（**需先在 Router 上创建好公网地址池**）。



NAT转换映射表		
方向	进入路由器	离开路由器
Outbound	10.1.1.100: 1025	162.105.178.65: 16384
Inbound	162.105.178.65: 16384	10.1.1.100: 1025
Outbound	10.1.1.200: 1028	162.105.178.65: 16400
Inbound	162.105.178.65: 16400	10.1.1.200: 1028

图 6-2　NAPT 实现原理示意图

① 假设先是私网侧 HostA 主机要访问公网侧 Server，向 Router 发送请求报文（即 Outbound 方向），此时报文中的源地址是 HostA 的 IP 地址 10.1.1.100，源端口号 1025。

② Router 在收到来自 HostA 发来的请求报文后，从事先配置好的公网地址池中选取一对空闲的“公网 IP 地址:端口号”，建立与内网侧 HostA 发送的请求报文中的“源 IP 地址:源端口号”间的 NAPT 转换表项（同样包括正、反两个方向），然后依据正向 NAPT 表项查找结果将请求报文中的“源 IP 地址:源端口号”（10.1.1.100:1025）转换成对应的“公网 IP 地址:端口号”（162.105.178.65:16384）后向公网侧发送。即此时经过 Router 的 NAPT 转换后，发送的请求报文中的源 IP 地址为 162.105.178.65，源端口号为 16384，目的 IP 地址和目的端口号不变。

③ 公网侧 Server 在收到由 Router 转发的请求报文后，需要向 Router 发送响应报文（即 Inbound 方向），此时只须将收到的请求报文中的源 IP 地址、源端口和目的 IP 地址、目的端口对调即可，即此时报文中的目的 IP 地址和目的端口号就是收到的请求报文中的源 IP 地址和源端口（162.105.178.65:16384）。

④ 当 Router 收到来自 Server 的响应报文后，根据其中的“目的 IP 地址:目的端口号”查找反向 NAPT 表项，并依据查找结果将报文转换后向私网侧发送。此时，报文中的目的 IP 地址和目的端口又将转换成请求报文在到达 Router 前的源 IP 地址和源端口，即 10.1.1.100:1025。

此时，如果 HostB 主机也要访问公网中的 Server，当请求报文到达 Router 时，报文中的源 IP 地址和源端口号也将进行转换，且它仍然可以使用 HostA 原来使用过的公网 IP 地址，但所用的端口号一定要不同，假设由原来的（10.1.1.200:1028）转换为 162.105.178.65:16400。Server 发给 HostB 的响应报文在 Router 上目的 IP 地址和目的端

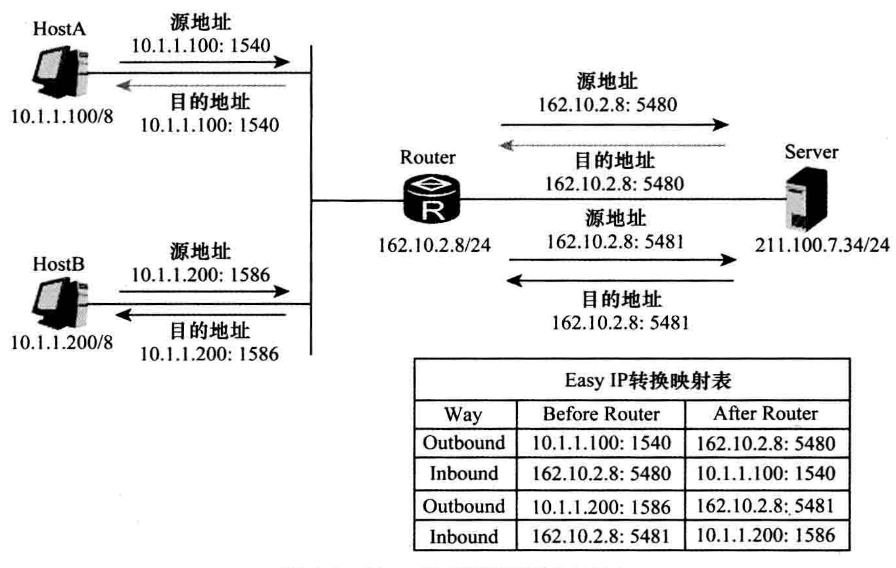
口也要经过转换，利用前面形成的 NATP 转换映射表进行逆向转换，即由原来的 162.105.178.65:16400 转换为 10.1.1.200:1028。

【经验之谈】从以上 NAPT 实现原理分析可以看出，**请求报文中转换的仅是源 IP 地址和源端口号**（目的 IP 地址和目的端口号不变），**即仅需关心源 IP 地址和源端口号；而响应报文中转换的是目的 IP 地址和目的端口号**（源 IP 地址和源端口号不变），**即仅需关心目的 IP 地址和目的端口号**。不同私网主机可以转换成同一个公网 IP 地址，**但转换后的端口号必须不一样**。

6.1.4 Easy IP 实现原理

Easy IP 方式的实现原理与上节介绍的地址池 NAPT 转换原理类似，可以算是 NAPT 的一种特例，不同的是 Easy IP 方式可以实现**自动根据路由器上 WAN 接口的公网 IP 地址实现与私网 IP 地址之间的映射（无需创建公网地址池）**。

Easy IP 主要应用于将路由器 WAN 接口 IP 地址作为要被映射的公网 IP 地址的情形，特别适合小型局域网接入 Internet 的情况。这里的小型局域网主要指中小型网吧、小型办公室等环境，一般具有以下特点：内部主机较少、出接口通过拨号方式获得临时（或固定）公网 IP 地址以供内部主机访问 Internet。图 6-3 所示为 Easy IP 方式的实现原理，具体过程如下。



Easy IP转换映射表

Way	Before Router	After Router
Outbound	10.1.1.100: 1540	162.10.2.8: 5480
Inbound	162.10.2.8: 5480	10.1.1.100: 1540
Outbound	10.1.1.200: 1586	162.10.2.8: 5481
Inbound	162.10.2.8: 5481	10.1.1.200: 1586

图 6-3　Easy IP 实现原理示意图

① 假设私网中的 Host A 主机要访问公网的 Server，首先要向 Router 发送一个请求报文（即 Outbound 方向），此时报文中的源地址是 10.1.1.100，端口号 1540。

② Router 在收到请求报文后自动利用公网侧 WAN 接口临时或者固定的“公网 IP 地址:端口号”（162.10.2.8:5480），建立与内网侧报文“源 IP 地址:源端口号”间的 Easy IP 转换表项（也包括正、反两个方向），并依据正向 Easy IP 表项的查找结果将报文转换后向公网侧发送。此时，转换后的报文源地址和源端口号由原来的（10.1.1.100:1540）转换成了（162.10.2.8:5480）。

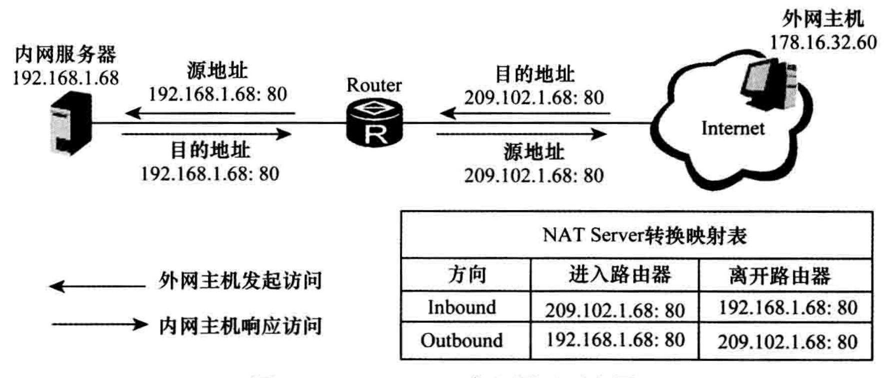
③ Server 在收到请求报文后需要向 Router 发送响应报文（即 Inbound 方向），此时只须将收到的请求报文中的源 IP 地址、源端口号和目的 IP 地址、目的端口号对调即可，即此时的响应报文中的目的 IP 地址、目的端口号为 162.10.2.8:5480。

④ Router 在收到公网侧 Server 的回应报文后，根据其"目的 IP 地址:目的端口号"查找反向 Easy IP 表项，并依据查找结果将报文转换后向内网侧发送。即转换后的报文中的目的 IP 地址为 10.1.1.100，目的端口号为 1540，与 Host A 发送请求报文中的源 IP 地址和源端口完全一样。

如果私网中的 Host B 也要访问公网，则它所利用的公网 IP 地址与 Host A 一样，都是路由器 WAN 口的公网 IP 地址，但转换时所用的端口号一定要与 Host A 转换时所用的端口不一样。

6.1.5 NAT Server 实现原理

NAT Server 用于外网用户需要使用固定公网 IP 地址访问内部服务器的情形。它通过事先配置好的服务器的"公网 IP 地址+端口号"与服务器的"私网 IP 地址+端口号"间的静态映射关系来实现。图 6-4 所示为 NAT Server 的实现原理，具体过程如下（**要先在 Router 上配置好静态的 NAT Server 转换映射表**）。



NAT Server转换映射表		
方向	进入路由器	离开路由器
Inbound	209.102.1.68: 80	192.168.1.68: 80
Outbound	192.168.1.68: 80	209.102.1.68: 80

图 6-4　NAT Server 实现原理示意图

① Router 在收到外网用户发起的访问请求报文后（即 Inbound 方向），根据该请求的"目的 IP 地址:端口号"查找 NAT Server 转换映射表，找出对应的"私网 IP 地址:端口号"，然后用查找的结果直接替换报文的"目的 IP 地址:端口号"，最后向内网侧发送。如本示例中外网主机发送的请求报文中目的 IP 地址是 209.102.1.68，端口号为 80，经 Router 转换后的目的 IP 地址和端口号为 192.168.1.68:80。

② 内网服务器在收到由 Router 转发的请求报文后，向 Router 发送响应报文（即 Outbound 方向），此时报文中的源 IP 地址、端口号与目的 IP 地址、端口号与所收到的请求报文中的完全对调，即响应报文中的源 IP 地址和端口号为前面的 192.168.1.68:80。

③ Router 在收到内网服务器的回应报文后，又会根据该响应报文中的"源 IP 地址:源端口号"查找 NAT Server 转换表项，找出对应的"公网 IP 地址:端口号"，然后用查找结果替换报文的"源 IP 地址:源端口号"。如本示例中内网服务器响应外网主机的报文的

源 IP 地址和端口号是 192.168.1.68:80，经 Router 转换后的源 IP 地址和端口号为 209.102.1.68:80。

【经验之谈】从以上 NAT Server 实现原理可以看出，由外网向内网服务器发送的**请求报文中转换的仅是其目的 IP 地址和目的端口号**（源 IP 地址和源端口号不变），**即仅需关心目的 IP 地址和目的端口号**；而从内网向外网发送的**响应报文中转换的仅是其源 IP 地址和源端口号**（目的 IP 地址和目的端口号不变），**即仅需关心源 IP 地址和源端口号**。两个方向所转换的 IP 地址和端口号是相反的。

再综合前面 6.1.1 小节和 6.1.2 小节可以得出，NAT 中**凡是由内网向外网发送的报文**（不管是请求报文，还是响应报文），**在 NAT 路由器上转换的都是源 IP 地址**（或者同时包括源端口号），而**凡是由外网向内网发送的报文**（也不管是请求报文，还是响应报文），**在 NAT 路由器上转换的都是目的 IP 地址**（或者同时包括源目的端口号）。

6.1.6 静态 NAT/NAPT

静态 NAT 是指在进行 NAT 转换时，内部网络主机的 IP 地址与公网 IP 地址是一对一静态绑定的，且每个公网 IP 只会分配给固定的内网主机转换使用。这与 6.1.1 小节介绍的 Basic NAT 实现原理基本一样，**不同的只是这里先要在 NAT 路由器上配置好静态 NAT 转换映射表，而不仅是地址池。**

静态 NAPT 是指“内部网络主机的私网 IP 地址+协议号+端口号”与“公网 IP 地址+协议号+端口号”是一对一静态绑定的，静态 NAPT 中的公网 IP 可以为多个私网 IP 使用。这与 6.1.1 小节介绍的 NAPT 的实现原理基本一样，**不同的也是这里先要在 NAT 路由器上配置好静态 NAPT 转换映射表，也不仅是地址池。**

静态 NAT/NAPT 还支持将指定的一个范围的私网主机 IP 地址转换为指定的公网范围内的主机 IP 地址。当内部主机访问外部网络时，如果该主机地址在指定的内部主机地址范围内，则会被转换为对应的公网地址；同样，当公网主机对内部主机进行访问时，如果该公网主机 IP 经过 NAT 转换后对应的私网 IP 地址在指定的内部主机地址范围内，则也可以直接访问到内部主机。

6.1.7 NAT 与路由的本质区别

许多读者对 NAT 和路由的区别不是很清楚，总想不通为什么有了路由还要 NAT，或者反过来问。其实这两种技术主要存在实现机制和主要应用两个方面的本质区别。

1. 实现机制不同

NAT 是通过**解决两个网络间互访的“身份”问题**来实现两个网络的主机的互访，即通过将报文中的源 IP 地址或者目的 IP 地址，或者两者同时（仅在两个网络中使用了同一网段的情况下）转换为对方网络的 IP 地址来实现两个网络中的主机互访。这里报文中的 IP 地址转换就相当于“身份”的转换，即使一个网络中的主机具有访问对方网络的合法“身份”。

路由则是通过**解决两个网络互访“渠道”问题**来实现两个网络的主机的互访，即建立一条互访的“路径”（即路由表）来实现双方主机的互访，而双方传输报文中的源 IP 地址和目的 IP 地址都是不变的，也就是双方的“身份”并没有经过转换。

2. 主要应用不同

之所以NAT要解决互访“身份”问题，是因为NAT主要应用于内部局域主机与Internet主机互访的情形（**当然NAT也可以实现两个局域网之间的互联，但这不是NAT的主要应用**），以便解决当前公网IPv4地址严重不足的问题。因为在局域网和Internet中使用的IP地址类型是完全不同的（局域网中使用的是“私网”IP地址，而Internet中使用的是“公网”IP地址），且彼此不识别。另外，在局域网与Internet的互联中根本无法也不可能建立一个双向互访的具体路由表，一则还是因为私网IP地址在Internet无法识别，不可能与公网IP地址之间直接建立路由，再则因为Internet不是单一IP网段的网络，包括处于各个网段的服务器主机。通过NAT就非常容易实现，只要你把私网IP地址转换成你拥有的一个公网IP地址，就可以以这个公网IP地址的身份实现对应权限的Internet访问了。

路由之所以会选择通过建立路径来实现两个网络的主机的互访，那是因为路由主要都是使用私网IP地址、有明确IP网段的局域网之间的互联。因为它们所使用的IP地址都是同种类型，彼此是可识别的，所以也就不存在“身份”问题，不需要在报文中经过IP地址转换。而且路由功能更强大，它不仅可以实现像NAT那样直连在同一路由器的两个网络间的互访，还可以比较简单地实现非直连在同一路由器上、多级网络间的互访。

6.2 NAT扩展技术及主要应用

在AR G3系列路由器中，为了满足一些特殊应用环境中的NAT应用，还提供了几种扩展NAT技术，它们是NAT ALG（Application Level Gateway，应用层网关）、DNS Mapping（DNS映射）、NAT关联VPN、两次NAT、NAT过滤和NAT映射。但要说明的是，**这些NAT扩展技术也必须是在以上介绍的静态NAT、动态NAT和NAT Server这三种NAT特性中应用，不能单独配置应用**。下面分别进行介绍。

6.2.1 NAT ALG

NAT和NAPT只能对IP报文的头部地址和TCP/UDP头部的端口信息进行转换，没有对来自应用层数据中可能包括的IP地址和端口信息（如FTP、DNS、SIP等数据报文中就包括了这些信息）进行对应转换。这样一来，当数据到达对方应用层后，所看到的仍是没有经过相应转换的应用层地址和端口信息。这样在对端应用层发送响应报文时，采用的就是没有经过相应地址转换的源端信息作为目的地址和端口信息（是公网IP地址和公网端口号），结果肯定是响应报文无法到达配置了私网IP地址和私网端口号的源端。

解决这些特殊应用层协议的NAT转换问题的方法就是在NAT实现中使用ALG功能。ALG会对特定的应用层协议进行转换，在对这些特定的应用层协议进行NAT转换过程中，利用所形成的NAT映射表（可以是静态配置的，也可以是根据配置的地址池动态形成的）信息来同时改变封装在IP报文数据部分中的地址和端口信息，同时允许这些在数据部分带有不可识别的私网地址和端口信息的应用层协议报文可以穿越NAT设备进行传输，**相当于屏蔽了报文中的私网地址信息**。

例如，一个使用内部 IP 地址的 FTP 服务器可能在和外部网络主机建立会话的过程中需要将自己的 IP 地址发送给对方。而这个地址信息是放在 IP 报文的数据部分，NAT 无法对它进行转换。当外部网络主机接收了这个私有地址并使用它时，FTP 服务器将表现为不可达。

目前支持 ALG 功能的协议包括 DNS、FTP、ICMP、SIP、PPTP 和 RTSP。**ALG 可全面应用于静态 NAT、动态 NAT 和 NAT Server 这三种 NAT 特性中。**

6.2.2 DNS Mapping

在某些应用中，私网用户希望通过域名访问时位于同一私网的内部服务器，而此时用于解析内部服务器的 DNS 服务器却位于公网。这样，当用户访问时首先会通过 NAT 处位于公网的 DNS 服务器发出域名解析请求，公网中的 DNS 服务器发出响应报文时在数据部分携带的是内部服务器对应的公网 IP 地址（也就是在 NAT Server 上配置的公网映射 IP 地址）。这时如果在 NAT Server 上没将 DNS 服务器解析的公网 IP 替换成内部服务器对应的私网 IP 地址，私网用户将无法通过域名访问到内部服务器，因为此时私网用户访问的是公网 IP 地址，而实际上服务器是在私网中，IP 地址为私网 IP 地址，自然就访问不了。

这个问题可以使用 DNS Mapping 方式来解决。其实 DNS Mapping 技术是 6.2.1 小节介绍的 DNS ALG 技术的一种补充技术。在 DNS ALG 中，报文中的 IP 地址信息直接通过 NAT 映射表进行替换，而 DNS Mapping 在替换报文数据部分的地址信息时先要通过查找专门配置的“域名-公网 IP 地址-公网端口-协议类型”映射表，找到对应域名所映射的公网 IP 地址后使用 NAT 地址映射表对数据部分的地址信息（还可能包括端口、协议）用内部服务器的私网地址信息（同样还可能包括端口、协议）进行替换。建立“域名-公网 IP 地址-公网端口-协议类型”映射表的目录是建立内部服务器的公网域名与其公网地址信息间的对应关系。

【经验之谈】这里的 DNS Mapping 与 6.2.1 小节介绍的 NAT ALG 有相似之处，都是用来解决一些应用协议报文中数据部分地址信息转换的问题,但两者之间又有较大不同，主要体现在用来替换的私网 IP 地址可能不一样。另外，ALG 功能还允许数据部分为私网信息的报文穿越 NAT 设备，在不同网络中传输，DNS Mapping 本身没这种功能。所以 **DNS Mapping 必须同时结合 ALG DNS 才能最终生效**，否则在数据部分为私网地址和端口信息的报文是不能穿越 NAT 设备进行传输的。当然，DNS Mapping 是仅应用于 DNS 应用中，不能应用于 ALG 中还包括的 FTP、RSTP 等之类的应用中。

在地址和端口信息转换方面，NAT ALG 中是直接利用静态配置，或者动态形成的公网 IP 地址与私网 IP 地址 NAT 映射表中的私网 IP 地址**同时替换报文中 IP 报头中的目的 IP 地址和数据部分中的公网 IP 地址，所以替换的私网 IP 地址与发起访问的主机的私网 IP 地址是绝对一致的**。DNS Mapping 中是通过事先配置的“域名-公网 IP 地址-公网端口-协议类型”映射表查找对应公网 IP 地址所对应的私网 IP 地址（或同时包括端口、协议信息）进行替换的；报文中的 IP 报头部分的目的 IP 地址是通过 NAT 地址映射表（在静态 NAT 或者 NAT Server 中配置的）进行替换的。**这时数据部分替换的私网 IP 地址与 IP 报头部分替换的私网目的 IP 地址可能一样（在 NAT Server 应用中），也可能不一样（在静态 NAT 应用中）。**

图 6-5 所示为 DNS Mapping 的基本原理。私网用户 Host 希望通过域名方式访问 Web

服务器，Router 作为 NAT Server。当 Router 设备收到 DNS 服务器发出的响应报文后，先根据其中携带的域名（www.test.com）查找“域名-公网 IP 地址-公网端口-协议类型”映射表，找到对应域名所用的公网 IP 地址，然后根据 NAT 上配置公网 IP 地址与私网 IP 地址的静态映射关系，将报文中的目的 IP 地址和数据部分的服务器公网 IP 地址（或同时将端口）替换成为 Web 服务器的私网 IP 地址 10.1.1.200（或同时替换端口）。这样，Host 收到的 DNS 响应报文中就携带了 Web 服务器的私网 IP 地址，从而可以通过域名来访问 Web 服务器了。

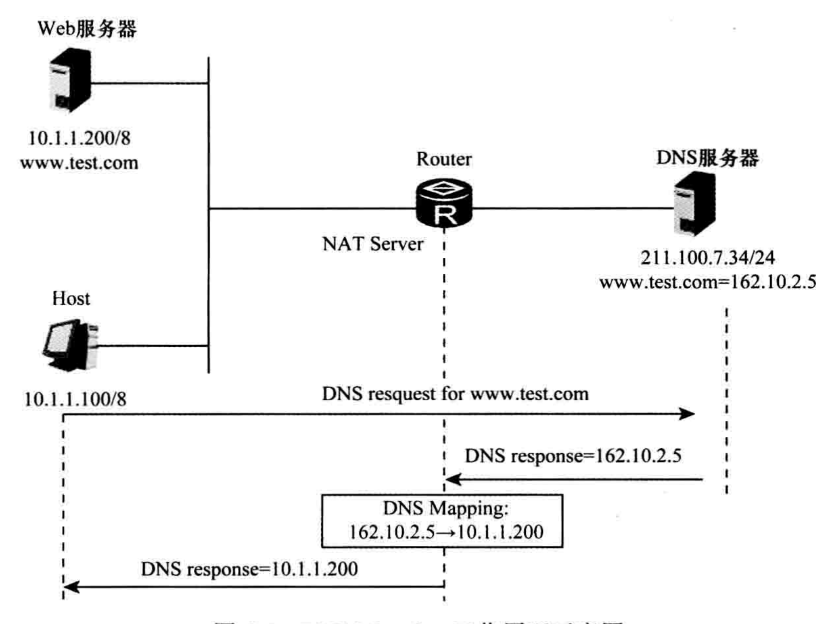


图 6-5　DNS Mapping 工作原理示意图

DNS Mapping 仅可应用于静态 NAT 和 NAT Server 中，不能应用于动态 NAT 中，这也是它与 ALG 技术的一种明显区别。

6.2.3　NAT 关联 VPN

NAT 不仅可以使内部网络的用户访问外部网络，还允许内部网络中分属于不同 VPN 的用户通过同一个出口访问外部网络，解决内部网络中 IP 地址重叠的 VPN 同时访问外网主机的问题；NAT 还支持 VPN 关联的 NAT Server，允许外部网络中的主机访问内网中分属不同 VPN 的服务器，同时支持内网多个 VPN 地址重叠的场景。

1. VPN 关联的源 NAT

VPN 关联的源 NAT 就是指前面所说的**内部网络中分属于不同 VPN 的用户通过同一个 NAT 出口访问外部网络，仅可应用于静态 NAT 中**。

图 6-6 对 VPN 关联的源 NAT 的实现原理进行了描述，具体过程如下。

① VPN 1 内的主机 A 和 VPN 2 内的主机 B 地址重叠，都为私网地址 10.1.1.1，都要同时访问外部网络的一个服务器。

② Router 在做源 NAT 时，将内部 VPN 作为一个 NAT 的匹配条件，将主机 A 发出报文的源 IP 转换为 202.1.1.1，将主机 B 发出报文的源 IP 转换为 202.1.2.1，同时在建立

的 NAT 转换表中，记录用户的 VPN 信息。

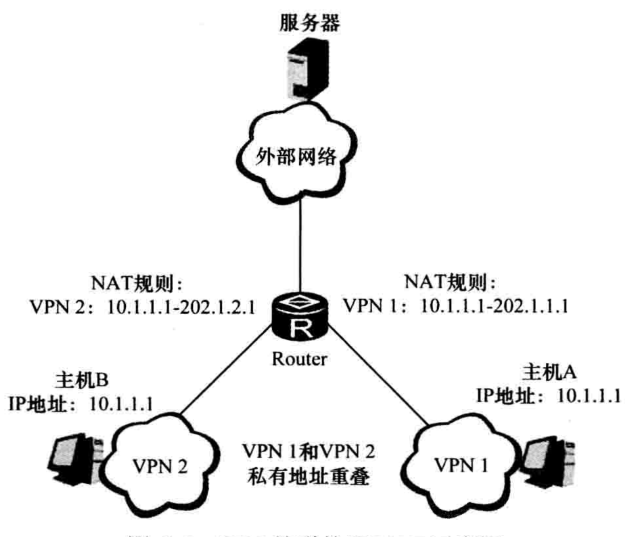


图 6-6 VPN 关联的源 NAT 示意图

③ 同样，当外部网络服务器回应内部网络主机 A 和主机 B 的报文经过 Router 时，根据已建立的 NAT 映射表，NAT 模块将发往主机 A 报文的目的 IP 从 202.1.1.1 转换为 10.1.1.1，然后发往 VPN 1 的目的主机；将发往主机 B 报文的目的 IP 从 202.1.2.1 转换为 10.1.1.1，然后发往 VPN 2 的目的主机。

2. VPN 关联的 NAT Server

VPN 关联的 NAT Server 是指**外网主机通过 NAT 技术访问内网中分属不同 VPN 的服务器，仅可应用于 NAT Server 中。**

如图 6-7 所示，VPN 1 内 Server A 和 VPN 2 内的 Server B 的地址都是 10.1.1.1；使用 202.1.10.1 作为 VPN 1 内的 Server A 的外部地址，使用 202.1.20.1 作为 VPN 2 内的 Server B 的外部地址。这样，外部网络的用户使用 202.1.10.1 就可以访问 VPN 1 提供的服务，使用 202.1.20.1 就可以访问 VPN 2 提供的服务。

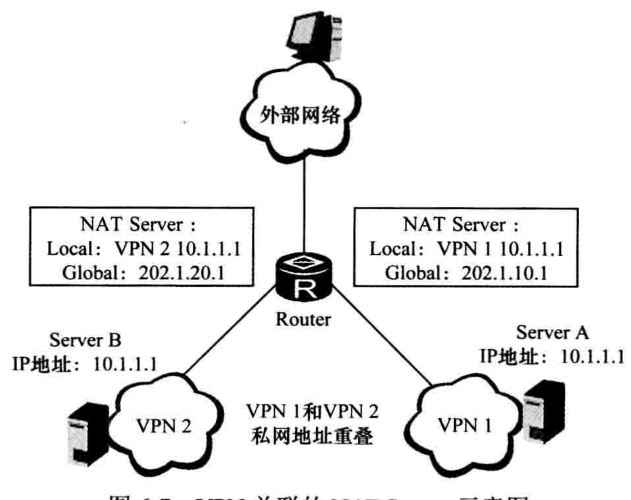


图 6-7 VPN 关联的 NAT Server 示意图

VPN 关联的 NAT Server 的实现方式如下。

① 外部网络的主机访问 VPN 1 内的 Server A 时的报文目的 IP 是 202.1.10.1；访问 VPN 2 内的 Server B 时的报文目的 IP 是 202.1.20.1。

② Router 在充当 NAT Server 时，根据报文的目的 IP 及 VPN 信息进行判断，将目的 IP 是 202.1.10.1 的报文的目的 IP 转换为 10.1.1.1，然后发往 VPN 1 的目的 Server A；将目的 IP 是 202.1.20.1 的报文的目的 IP 转换为 10.1.1.1，然后发往 VPN 2 的目的 Server B；同时在新建的 NAT 映射表中，记录下关联的 VPN 信息。

③ 当内部 Server A 和 B 回应外部网络主机的报文经过 Router 时，根据已建立的 NAT 映射表，NAT 模块将从 Server A 发出的报文的源 IP 从 10.1.1.1 转换为 202.1.10.1，再发往外部网络；将从 Server B 发出的报文的源 IP 从 10.1.1.1 转换为 202.1.20.1，再发往外部网络。

6.2.4 两次 NAT

两次 NAT 是指源 IP 地址和目的 IP 地址同时转换（前面介绍的 NAT 技术都是一个方向仅转换源 IP 地址或者目的 IP 地址），该技术应用于内部网络主机地址与外部网络上主机地址重叠的情况。它的设计思想就是通过一个中间的多个公网 IP 地址来分别对双向的源和目的 IP 地址进行转换。**两次 NAT 可全面应用于静态 NAT、动态 NAT 和 NAT Server 这三种 NAT 特性中。**

图 6-8 所示为两次 NAT 转换的过程，图中分别位于内、外网的 Host A 和 Host B 的 IP 网段是一样的，且本示例中 IP 地址都一样。具体转换原理如下（假设内外部网络地址均为 1.1.1.0/24）。

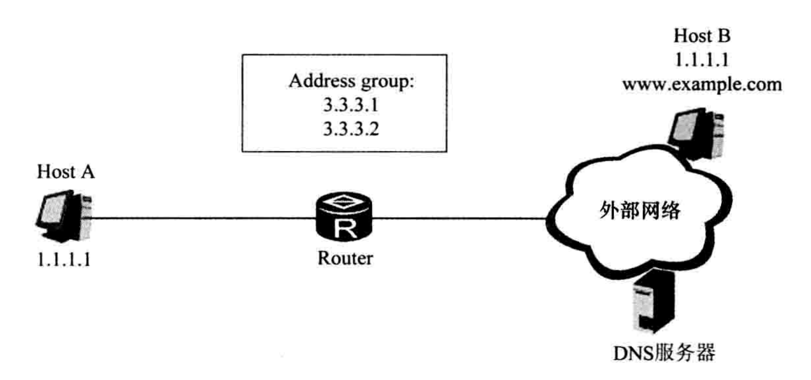


图 6-8 两次 NAT 转换示意图

① 内网 Host A 要访问地址重叠的外部网络 Host B，首先 Host A 会向位于外部网络的 DNS 服务器发送访问外网 Host B 的 DNS 解析请求，DNS 服务器应答 Host B 的 IP 地址为 1.1.1.1。

② DNS 应答报文在经过 Router 时，通过 DNS ALG 将 DNS 应答报文数据部分中的重叠地址 1.1.1.1 转换为唯一的临时地址 3.3.3.1，然后转发给 Host A。

③ Host A 获取了 Host B 的 IP 地址（其实是转换后的 IP 地址 3.3.3.1）后，开始访问 Host B，目的 IP 为临时地址 3.3.3.1。

④ 请求报文在到达 Router 时，先进行正常的 NAT Outbound 转换，将报文中的源 IP 地址转换为源 NAT 地址池中的地址 3.3.3.2；同时 Router 检查到此时报文中的目的 IP 地址 3.3.3.1 与转换后的源 IP 地址 3.3.3.2 重叠，于是再进行目的 IP 地址转换，将报文的目的 IP 地址 3.3.3.1 转换为 Host B 的真实地址 1.1.1.1，最后将报文转发到 Host B。

⑤ Host B 回应 Host A 的访问请求后发出响应报文，其中的目的 IP 为 Host A 的 NAT Outbound 地址池地址 3.3.3.2，源 IP 为 Host B 的地址 1.1.1.1。

⑥ 响应报文在到达 Router 时，先进行正常的 NAT Inbound 转换，将报文中的目的 IP 地址从源 NAT 地址池地址中的地址 3.3.3.2 转换为 Host A 的内网地址 1.1.1.1；同时，Router 检查到此时报文中的源 IP 地址又与目的 IP 地址重叠，于是再进行源 IP 地址转换，将报文的源 IP 地址 1.1.1.1 转换为对应的临时地址 3.3.3.1，再将报文转发到 Host A。

考虑到内网有多个 VPN 的场景，且内网多个 VPN 的地址一样的情形，还可在路由器配置 DNS ALG 的同时增加内网 VPN 信息作为重叠地址池到临时地址的映射关系匹配条件之一。如图 6-9 所示，内网多 VPN 情况下的两次 NAT 转换过程和以上介绍的两次 NAT 转换的过程类似，只是 VPN A 中的 Host A 转换为临时地址 3.3.3.1，而 VPN B 中的 Host B 转换为临时地址 4.4.4.1。

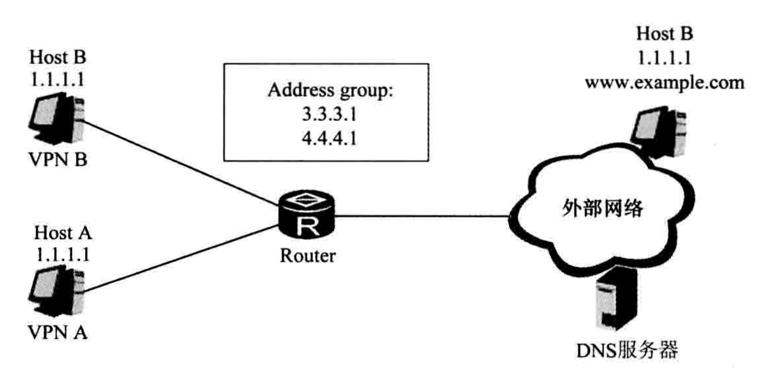


图 6-9　内网多 VPN 情况下的两次 NAT 示意图

6.2.5　NAT 过滤和 NAT 映射

NAT 过滤功能可以让 NAT 设备**对外网发到内网的流量**进行过滤；NAT 映射功能可以**让内网中的一组主机通过 NAT 映射表映射到一个公网 IP 地址**，共享这一个公网 IP 地址，所有不同的信息流看起来好像来源于同一个 IP 地址。**NAT 过滤和映射均可全面应用于静态 NAT、动态 NAT 和 NAT Server 这三种 NAT 特性中。**

1. NAT 过滤

NAT 过滤是指 NAT 设备对外网发到内网的流量进行过滤。根据过滤的条件，NAT 过滤分为三种类型。

① 与外部地址无关的 NAT 过滤行为。

② 与外部地址相关的 NAT 过滤行为。

③ 与外部地址和端口都相关的 NAT 过滤行为。

NAT 过滤的典型应用场景如图 6-10 所示。图中私网用户 PC-1 通过 NAT 设备与外网用户 PC-2、PC-3 进行通信。数据报文 1 代表私网主机 PC-1 访问公网 PC-2 的报文，此时 PC-1 使用的源端口号为 1111，访问 PC-2 的目的端口号为 2222；经过 NAT 设备时，源 IP 地址由 PC-1 的 IP 地址 10.1.1.1 转换为 202.169.10.1。

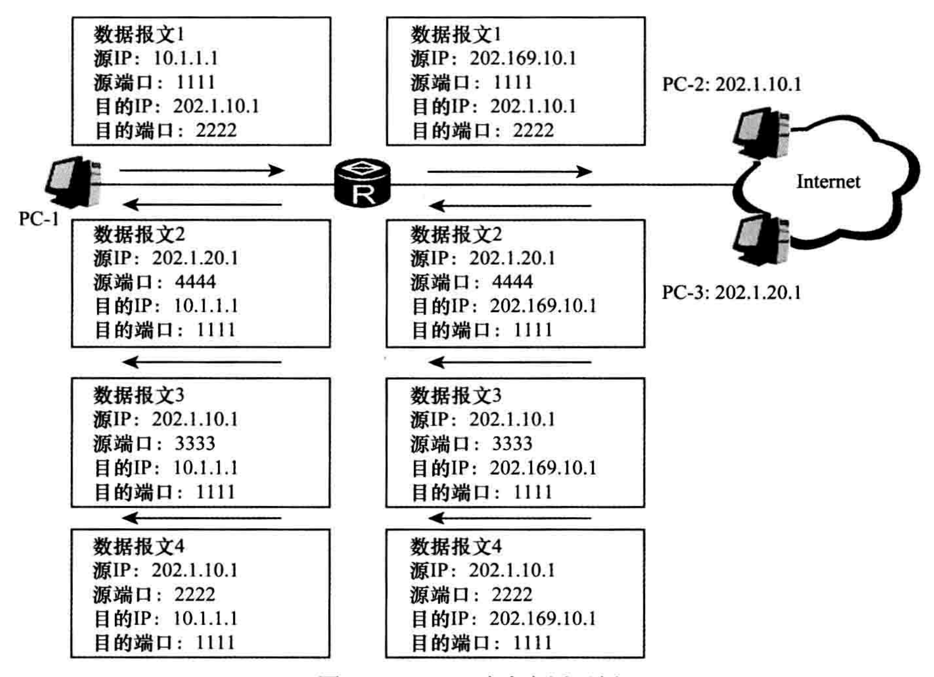


图 6-10 NAT 过滤应用示例

在私网主机向某公网主机发起访问后，公网主机发向私网主机的流量经过 NAT 设备时需要进行过滤。数据报文 2、数据报文 3 和数据报文 4 代表三种场景，分别对应上述三种 NAT 过滤类型。

① 数据报文 2 代表公网主机 PC-3（与前面的数据报文 1 的目的地址不同，**证明它不是 PC-1 要访问的对象**）访问私网主机 PC-1 的报文，此时目的端口号为 1111。这种情况下，只有在 NAT 设备上配置了外部地址无关的 NAT 过滤行为才会允许该报文通过（因为 PC-3 不是 PC-1 要访问的对象），否则被 NAT 设备过滤掉。

② 数据报文 3 代表公网主机 PC-2（与前面的数据报文 1 的目的地址相同）访问私网主机 PC-1 的报文，此时目的端口号为 1111，源端口号为 3333（与数据报文 1 的目的端口不同，**证明 PC-2 是换了端口号对 PC-1 进行访问的**）。这种情况下，只有配置了外部地址相关的 NAT 过滤行为，或者配置了外部地址无关的 NAT 过滤行为（**均不涉及端口号**），才会允许该报文通过，否则被 NAT 设备过滤掉。

③ 数据报文 4 代表公网服务器 PC-2（与数据报文 1 的目的地址相同）访问私网主机 PC-1 的报文，此时目的端口号为 1111，源端口号为 2222（与数据报文 1 的目的端口相同，**证明 PC-2 没有更换端口，直接对 PC-1 进行访问**）。这属于外部地址和端口都相

关的 NAT 过滤行为，是缺省的过滤行为，不配置或者配置任何类型的 NAT 过滤行为，都允许此报文通过，不会被过滤掉。

2. NAT 映射

NAT 映射是 NAT 设备对**内网发到外网的流量**进行的映射，可以使得一组内网主机共享唯一的外部地址对外进行通信。在 Internet 中使用 NAT 映射功能后，可使所有来自不同内网主机的信息流看起来好像来源于同一个 IP 地址，便于整体监控内网到外网的数据流。当位于内部网络中的主机通过 NAT 设备向外部主机发起会话请求时，NAT 设备就会查询 NAT 表，看是否有相关会话记录，如果有相关记录，就会将内部 IP 地址及端口同时进行转换，再转发出去；如果没有相关记录，进行 IP 地址和端口转换的同时，还会在 NAT 表增加一条该会话的记录。

根据不同的映射条件，NAT 映射包括以下三种类型。

① 外部地址无关的映射：对相同的内部 IP 地址和端口号使用相同的公网 IP 地址和公网端口号进行映射，**不考虑所访问的外部 IP 地址**。

② 外部地址相关的映射：对相同的内部 IP 地址和端口号，**访问相同的外部 IP 地址**时使用相同的公网端口进行映射。

③ 外部地址和端口相关的映射：对相同的内部 IP 地址和端口号，**访问相同的外部 IP 地址和端口号**时使用相同的公网端口号进行映射。

在 AR G3 系列路由器中，仅支持外部地址无关、外部地址和端口相关的映射，**不支持外部地址相关的映射**。

6.2.6 NAT 的主要应用

NAT 的应用非常广泛，也是路由器的一项非常重要功能（目前三层交换机均不具备 NAT 的功能）。本节介绍几种典型的 NAT 应用。

1. 私网主机访问公网服务器

在许多小区、学校和企业的内网规划中，由于公网 IP 地址资源有限，内网用户实际使用的都是私网 IP 地址上网。在这种情况下，可以使用 NAT 技术来实现私网用户对公网的访问。如图 6-11 所示，通过在路由器上配置 Easy IP 就可以实现私网主机访问公网服务器的目的。有关 Easy IP 的实现原理参见 6.1.4 小节。

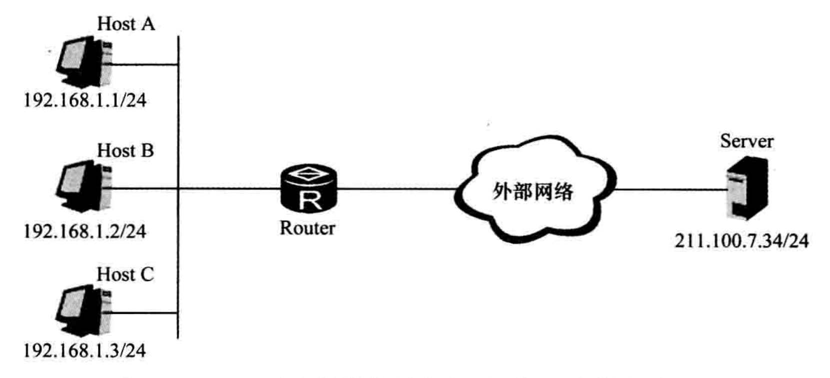


图 6-11　NAT 在私网主机访问公网服务器中的应用示例

2. 公网主机访问私网服务器

在某些场合，私网内部有一些服务器需要向公网提供服务，比如一些位于私网内的 Web 服务器、FTP 服务器等，NAT 可以支持这样的应用。如图 6-12 所示，通过配置 NAT Server，即定义"公网 IP 地址:端口号"与"私网 IP 地址:端口号"间的映射关系，使位于公网的主机能够通过该映射关系访问到位于私网的服务器。有关 NAT Server 的实现原理参见 6.1.5 小节。

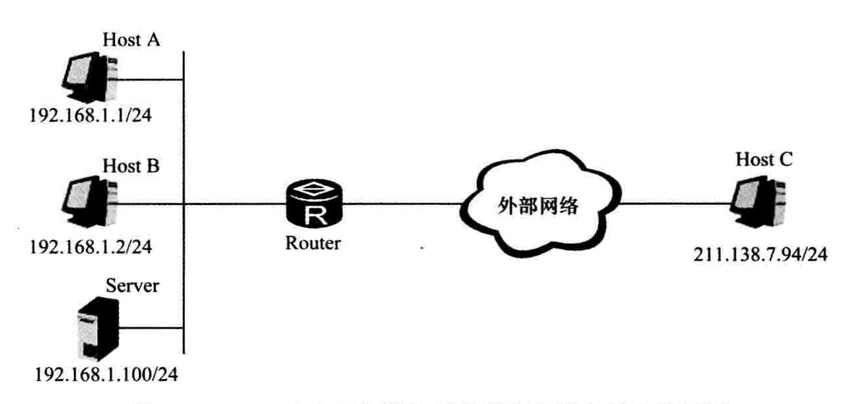


图 6-12　NAT 在公网主机访问私网服务器中的应用示例

3. 私网主机通过域名访问私网服务器

在某些场合，私网用户希望通过域名访问位于同一私网的内部服务器，而 DNS 服务器却位于公网，此时可通过同时配置 NAT Server 和 DNS Mapping 来实现。有关 NAT Server 的实现原理参见 6.1.4 小节；有关 DNS Mapping 的实现原理参见 6.2.2 小节。

如图 6-13 所示，通过配置 DNS Mapping 映射表，即定义"域名-公网 IP 地址-公网端口-协议类型"间的映射关系，将 DNS 响应报文中携带的公网 IP 地址替换成内部服务器的私网 IP 地址，从而使私网用户可以通过域名来访问该服务器。

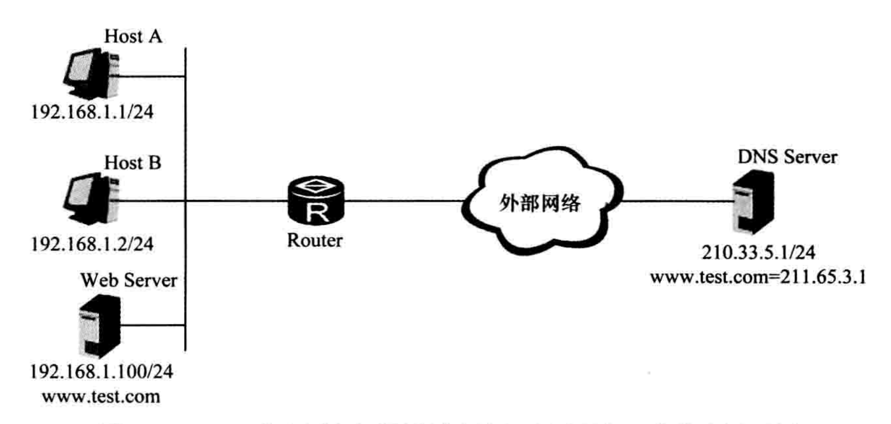


图 6-13　NAT 在私网主机通过域名访问私网服务器中的应用示例

4. NAT 多实例

当分属不同 MPLS VPN 的主机使用相同的私网地址，并通过同一个出口设备访问 Internet 时，NAT 多实例可使这些地址重叠的主机同时访问公网服务器。如图 6-14 所示，

尽管 HostA 和 HostB 具有相同的私网地址，但由于其分属不同的 VPN，通过使用 NAT 关联 VPN 技术，可以使 NAT 能够区分属于不同 VPN 的主机，允许二者同时访问公网服务器。有关的 NAT 关联 VPN 技术原理参见 6.2.3 小节。

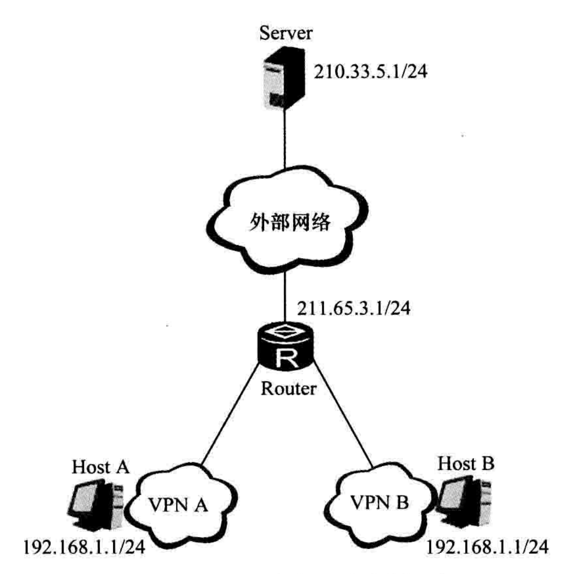


图 6-14　NAT 多实例的应用示例

6.3　配置动态 NAT

通过配置动态 NAT 可以动态地建立私网 IP 地址和公网 IP 地址的映射表项，实现私网用户访问公网，同时节省了所需拥有的公网 IP 地址数量。但在这里要特别说明的是，动态 NAT 包括前面介绍的一对一转换的 Basic NAT 和多对一转换的 NAPT、Easy IP 这三种 NAT 实现方式。

动态 NAT 的基本配置思想主要有三个方面：首先通过 ACL 指定允许使用 NAT 进行 IP 地址转换的用户范围，然后创建用于动态 NAT 地址转换的公网地址池，最后在 NAT 的出接口上把前面配置的 ACL 和公网地址池（如果采用的是 Easy IP 方式，则此时的公网地址池就是 NAT 出接口的 IP 地址）进行关联，相当于在 NAT 出接口上应用所配置的 ACL 和公网地址池。当然，还可以根据实际需要选择在 6.2 节介绍的其他 NAT 扩展技术。总体来说，动态 NAT 的主要配置任务如下（**各项配置任务之间没有严格的配置先后次序**）。

① 配置地址转换的 ACL 规则。

② 配置出接口的地址关联。

③（可选）使能 NAT ALG 功能。

④（可选）配置 NAT 过滤方式和映射模式。

⑤（可选）配置两次 NAT。

⑥（可选）配置 NAT 日志输出。

⑦（可选）配置NAT地址映射表项老化时间。

6.3.1 配置地址转换的ACL规则

这是一项必选配置任务，因为下面的出接口地址关联配置任务中必须要用到这里配置好的地址转换ACL，用于控制允许使用NAT进行地址转换的用户私网IP地址范围和网络应用范围。可根据实际情况选择配置基本ACL规则或者高级ACL规则指定允许使用NAT进行地址转换的用户主机源IP地址范围，可使用高级ACL同时限制使用NAT的通信协议类型，**但在规则中的地址范围方面仅可指定源IP地址，不能指定目的IP地址**。

说明 仅可在动态NAT中调用ACL来控制允许使用地址池进行地址转换的内部网络用户，在静态和NAT Server中因为相当于都静态配置了一对一的地址映射表，所以不需要ACL来控制。

动态NAT地址转换ACL的配置方法很简单，只需先在系统视图下使用**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]命令创建一个基本ACL或者高级ACL（如果仅需要过滤NAT应用报文中的源IP地址，则可配置基本ACL，否则要配置高级ACL），然后利用对应的基本ACL或者高级ACL中的**rule**命令配置相应的ACL规则。有关ACL的配置方法请参见配套图书《华为交换机学习指南》第9章。

【示例1】允许内部网络192.168.1.0/24网段的用户使用NAT地址池进行地址转换。

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 1 permit source 192.168.1.0 0.0.0.255
```

【示例2】允许内部网络192.168.1.10/24用户使用NAT地址池进行地址转换。

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 1 permit source 192.168.1.10 0
```

【示例3】允许内部网络192.168.1.0/24网段的用户在进行TCP通信时使用NAT地址池进行地址转换。

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule 3 permit tcp source 192.168.1.0 0.0.0.255
```

6.3.2 配置出接口的地址关联

这也是一项必选配置任务。出接口的地址关联就是把所创建的公网地址池（当采用Easy IP实现方式时为出接口的IP地址）与6.3.1小节配置的地址转换ACL在NAT出接口上进行关联。NAT地址池是用来存放用于对报文中为私网IP地址的源IP地址进行转换的公网IP地址集合。可以根据自己公网IP的规划情况选择以下的一种方式。

① 如果用户在配置了NAT设备出接口的IP地址和其他应用之后，还有空闲公网IP地址，可以配置单独的地址池。具体配置步骤如表6-1所示。

表 6-1　　地址池配置方式下的出接口地址关联配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**nat address-group** *group-index start-address end-address* 例如：[Huawei]**nat address-group** 1 202.110.10.10 202.110.10.15	配置 NAT 公网地址池。命令中的参数说明如下 • *group-index*：指定 NAT 地址池索引号，取值范围如下：AR150 系列为 0～3 的整数，AR200 和 AR1200 系列为 0～7 的整数，AR2200 系列为 0～15，AR3200 系列为 0～31 的整数 • *start-address*：指定地址池中的起始 IP 地址 • *end-address*：指定地址池中的结束 IP 地址 地址池的起始地址必须小于等于结束地址，且起始地址到结束地址之间的地址个数不能大于 255 缺省情况下，系统未配置 NAT 地址池，可用 **undo nat address-group** *group-index* 命令删除 NAT 地址池
3	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 NAT 路由器的**出接口**（只能是三层接口，但不包括 Loopback 接口和 NULL 接口），进入接口视图
4	**nat outbound** *acl-number* { **address-group** *group-index* [**no-pat**] | **interface** *interface-type interface-number* } 例如：[Huawei-GigabitEthernet1/0/0]**nat outbound** 2001 **address-group** 1 **no-pat**	将前面创建的 ACL 和第 2 步配置的公网地址池在以上出接口上进行关联，使符合 ACL 中规定的私网 IP 地址可以使用公网地址池进行地址转换。命令中的参数和选项说明如下 • *acl-number*：指定前面创建用于控制 NAT 应用的 ACL 编号 • **address-group** *group-index*：二选一参数，表示使用地址池的方式配置地址转换，指定要与 ACL 关联的地址池索引号 • **no-pat**：可选项，表示使用一对一的地址转换，只转换数据报文的地址而不转换端口信息 • **interface** *interface-type interface-number*：二选一参数，指定使用某个接口（**一般就是 NAT 的出接口**）的 IP 地址作为转换后的公网 IP 地址 可以在同一个接口上配置不同的地址转换关联。缺省情况下，系统未配置地址转换规则，可用 **undo nat outbound** *acl-number* [**address-group** *group-index* [**no-pat**] | **interface** *interface-type interface-number*]命令删除相应的地址转换规则

② 如果用户在配置了 NAT 设备出接口的 IP 地址和其他应用之后，已没有其他可用公网 IP 地址，则可以选择 Easy IP 方式，因为 Easy IP 可以借用 NAT 设备出接口的 IP 地址完成动态 NAT。具体配置步骤如表 6-2 所示。

表 6-2　　Easy IP 配置方式下的出接口地址关联配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 NAT 路由器的**出接口**（只能是三层接口，但不包括 Loopback 接口和 NULL 接口），进入接口视图

（续表）

步骤	命令	说明
3	**nat outbound** *acl-number* 例如：[Huawei-GigabitEthernet1/0/0]**nat outbound** 2001	配置Easy IP地址转换，直接使用出接口IP地址（**可以是静态的，也可以是动态的**）进行转换。参数*acl-number*用来指定前面已创建，要应用于控制NAT地址转换的ACL编号 缺省情况下，系统未配置Easy-IP地址转换，可用**undo nat outbound** *acl-number*命令删除相应的Easy IP方式的NAT地址转换规则

6.3.3 使能NAT ALG功能

这是一项可选配置任务，仅在要通过NAT设备进行DNS、FTP、SIP和RTSP等应用（如DNS服务器在公网中，需要在内网中使用域名访问位于内网的服务器时）时，需要配置NAT ALG功能。使能ALG功能可以使NAT设备识别被封装在报文数据部分的IP地址或端口信息，并根据动态形成的NAT地址（或同时包括端口号）映射表项进行替换，使报文正常穿越NAT。有关NAT ALG的工作原理参见6.2.1小节。

使能NAT ALG的方法很简单，仅需在系统视图下使用**nat alg { all | dns | ftp | rtsp | sip } enable**命令配置即可。缺省情况下，NAT ALG处于未使能状态，可用**undo nat alg { all | dns | ftp | rtsp | sip } enable**命令关闭对应应用协议的NAT ALG功能。

6.3.4 配置NAT过滤方式和映射模式

这也是一项可选配置任务，仅当网络中存在来自不同厂商的设备，且存在使用STUN（Simple Traversal of UDP Through NAT，通过NAT的UDP简单穿越）、TURN（raversal Using Relay NAT，使用中继NAT穿越）、ICE（Interactive Connectivity Establishment，交互式连通建立）技术的应用时才需要配置。因为不同厂商的NAT功能可能不完全一样，最终造成这些应用软件无法穿越NAT。

又因为以上这些应用技术广泛依赖于SIP（Session Initiation Protocol，会话初始化协议）代理等软件，而SIP又属于多通道应用，在功能实现时需要创建多个数据通道链接，因此为了保障多个通道的链接，必须配置NAT映射模式和过滤方式，只允许符合映射关系、过滤条件的报文通过。有关NAT过滤和NAT映射的工作原理参见6.2.5小节。

配置NAT过滤方式和映射模式的方法如表6-3所示。

表6-3　NAT过滤方式和映射模式的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei>**system-view**	进入系统视图
2	**nat mapping-mode endpoint-independent** [{ **tcp** | **udp** } [**dest-port** *port-number*]] 例如：[Huawei] **nat mapping-mode endpoint-independent**	配置NAT映射模式。命令中的参数和选项说明如下。 • **endpoint-independent**：指定NAT映射类型为与外部终端地址不相关的模式 • **tcp**：二选一选项，指定NAT映射应用于TCP通信 • **udp**：二选一选项，指定NAT映射应用于UDP通信 • **dest-port** *port-number*：可选参数，指定NAT映射应用的TCP或UDP的目的端口号，取值范围为1～65 535的整数

（续表）

步骤	命令	说明
2	**nat mapping-mode endpoint-independent** [{ **tcp** | **udp** } [**dest-port** *port-number*]] 例如：[Huawei] **nat mapping-mode endpoint-independent**	如果不指定 TCP 或者 UDP，以及不指定目的端口号，则表示 NAT 映射与传输协议和传输层端口均无关 缺省情况下，NAT 映射模式为与外部地址和端口相关的映射，可用 **undo nat mapping-mode endpoint-independent** [{ **tcp** | **udp** } [**dest-port** *port-number*]]命令取消已配置的对应 NAT 映射模式
3	**nat filter-mode** { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** } 例如：[Huawei] **nat filter-mode endpoint-dependent**	配置 NAT 过滤方式。命令中的选项说明如下 ● **endpoint-dependent**：多选一选项，指定 NAT 过滤与外部终端地址相关 ● **endpoint-independent**：多选一选项，指定 NAT 过滤与外部终端地址不相关 ● **endpoint-and-port-dependent**：多选一选项，指定 NAT 过滤与外部终端地址和端口同时相关 缺省情况下，NAT 过滤方式为 **endpoint-and-port-dependent**

6.3.5 配置两次 NAT

这也是一项可选配置任务，仅当内外网地址重叠（也就是属于同一 IP 网段）时才需要通过两次 NAT 来实现内外网的正常通信。此时内外网主机可以根据重叠地址池和临时地址池的映射关系，将重叠地址替换为临时地址后再进行 NAT 地址转换，以实现内外网的互访。重叠地址池用来指定内网哪些 IP 允许和外网重叠，只有属于重叠地址池的地址才会做两次 NAT；临时地址池指定了可用哪些临时 IP 地址来替换重叠地址池里的地址。

配置两次 NAT 就是要配置重叠地址池和临时地址池的映射关系，方法是在系统视图下使用 **nat overlap-address** *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]命令配置。命令中的参数说明如下。

① *map-index*：指定重叠地址池到临时地址池映射关系索引号，取值范围如下：AR150/150-S 系列为 0～3 的整数，AR200/200-S/1200/1200-S 系列为 0～7 的整数，AR2200/2200-S 系列为 0～15，AR3200 系列为 0～31 的整数。

② *overlappool-startaddress*：指定重叠地址池起始地址，各重叠地址池的地址不能有交集。

③ *temppool-startaddress*：临时地址池起始地址，各临时地址池的地址不能有交集。

④ **pool-length** *length*：指定以上两个相互关联的重叠地址池与临时地址池的长度，它们的长度是相等的，且地址一一对应，取值范围为 1～255 的整数。

⑤ **inside-vpn-instance** *inside-vpn-instance-name*：可选参数，指定要应用以上地址池映射的内网 VPN 实例名。

缺省情况下，系统未配置重叠地址池到临时地址池的映射，可用 **undo nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }命令删除已配置的指定或全部映射。当配置中的 VPN 实例删除时，两次 NAT 的配置也同步删除。

注意 配置好重叠地址池到临时地址池后的映射后还需要配置从 NAT 出接口到达临时地址的静态路由（目的 IP 地址为临时 IP 地址，出接口为 NAT 出接口，下一跳 IP 地址通常为运营商侧的公网 IP 地址），否则 NAT 流量仍然无法通过出接口发出去。

6.3.6　配置 NAT 日志输出

这也是一项可选配置任务。可根据实际需要在 NAT 设备上配置 NAT 日志输出功能，保存在进行 NAT 应用时所生成的信息记录。该记录包括报文的源 IP 地址、源端口、目的 IP 地址、目的端口、转换后的源 IP 地址、转换后的源端口以及 NAT 的时间信息和用户执行的操作等。网络管理员可以通过查看 NAT 日志实时定位用户通过 NAT 访问网络的情况，增强了网络的安全性。

配置 NAT 日志输出的步骤如表 6-4 所示。

表 6-4　　NAT 日志输出的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**firewall log session enable** 例如：[Huawei] **firewall log session enable**	使能防火墙流日志功能，包括通过定义 ACL 规则对符合条件的流所记录的日志以及对 NAT 转换的流所记录的日志 缺省情况下，防火墙日志功能未使能，可用 **undo firewall log enable** 命令去使能防火墙日志功能
3	**firewall log session nat enable** 例如：[Huawei]**firewall log session nat enable**	使能 NAT 类型的流日志功能，包括通过定义 ACL 规则对符合条件的流所记录的日志以及对 NAT 转换的流所记录的日志 缺省情况下，NAT 类型的流日志功能未使能，可用 **undo firewall log session nat enable** 命令去使能 NAT 类型的流日志功能
4	**info-center enable** 例如：[Huawei] **info-center enable**	（可选）使能信息中心功能。设备运行时，信息中心会通过信息的形式实时记录设备运行情况。只有使能了信息中心功能，系统才会向日志主机、控制台等方向输出系统信息。网络管理员可以存储和查阅输出信息为监控设备的运行情况和诊断网络故障提供依据 缺省情况下，**信息中心功能已处于使能状态**，故本步可选，可用 **undo info-center enable** 命令去使能信息中心功能。执行 **undo info-center enable** 命令行后，设备上产生的 Log、Trap 和 Debug 信息都不再记录，包括执行 **undo info-center enable** 命令产生的日志信息也不记录
5	**info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { language *language-name* |binary [*port*] } | { **vpn-instance** *vpn-instance-name* | **public-net** }] * 例如：[Huawei] **info-center loghost** 202.38.160.1 **channel** channel6	配置日志信息输出到日志主机所使用的通道。命令中的参数说明如下 • *ip-address*：指定日志主机的 IP 地址 • **channel** { *channel-number* | *channel-name* }：可多选参数，指定向日志主机发送信息所使用的信息通道，选择参数 *channel-number* 时指定通道号，取值范围为 0～9 的整数；选择参数 *channel-name* 时指定通道名称，1～30 个字符，区分大小写，只能由字母或数字组成，并且第一个字符只能为字母

（续表）

步骤	命令	说明
5	**info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { language *language-name* |binary [*port*] } | { **vpn-instance** *vpn-instance-name* | **public-net** }] * 例如：[Huawei] **info-center loghost** 202.38.160.1 **channel** channel6	● **facility** *local-number*：可多选参数，指定设置日志主机的记录工具，取值范围为 local0～local7。缺省值是 local7 ● **language** *language-name*|**binary** [*port*]：可多选参数，指定信息输出到日志主机所显示的语言模式（选择参数 **language** *language-name*|时，取值为 English）或指定向日志主机发送二进制形式的日志（选择参数 **binary** [*port*]时），并指定发送日志时所用的端口号（取值范围为 1～65 535 的整数，缺省值为 514） ● **vpn-instance** *vpn-instance-name* | **public-net**：：可多选参数，指定日志主机所在的 VPN 实例名（选择 **vpn-instance** *vpn-instance-name* 参数时）或者指定在公网中连接日志主机（选择 **public-net** 选项时） 系统最多可配置 8 个日志主机，实现日志主机间相互备份的功能。缺省情况下，不向日志主机输出信息，可用 **undo info-center loghost** *ip-address* [**vpn-instance** *vpn-instance-name*]命令取消向指定的日志主机输出信息

6.3.7 配置 NAT 地址映射表项老化时间

这也是一项可选配置任务，可根据需要为 NAT 地址映射表配置老化时间，以控制用户对 NAT 配置的使用，确保内、外网的通信安全。

配置 NAT 地址映射表项老化时间的方法也很简单，只须在系统视图下使用 **firewall-nat session { dns | ftp | ftp-data | http | icmp | tcp | tcp-proxy | udp | sip | sip-media | rtsp | rtsp-media }aging-time** *time-value* 命令配置即可。参数 *time-value* 的取值范围为 1～65 535 的整数秒。如果要配置多个会话表项的超时时间需要分别用本命令配置。

缺省情况下，各协议的老化时间为：DNS（120 s）、ftp（120 s）、ftp-data（120 s）、HTTP（120 s）、icmp（20 s）、tcp（600 s）、tcp-proxy（10 s）、udp（120 s）、sip（1 800 s）、sip-media（120 s）、rtsp（60 s）、rtsp-media（120 s），可用 **undo firewall-nat session { all | dns | ftp | ftp-data | http | icmp | tcp | tcp-proxy | udp | sip | sip-media | rtsp | rtsp-media } aging-time** 命令恢复对应会话表项的超时时间为缺省值。

6.3.8 动态 NAT 地址转换配置示例

本示例的拓扑结构如图 6-15 所示，某公司 A 区和 B 区的私网用户和 Internet 相连，路由器上出接口 GigabitEthernet3/0/0 的公网地址为 202.169.10.1/24，对端运营商侧地址为 202.169.10.2/24。A 区用户希望使用公网地址池中的地址（202.169.10.100～202.169.10.200），采用 NAT 方式替换 A 区内部的主机地址（网段为 192.168.20.0/24），访问 Internet；B 区用户希望结合 B 区的公网 IP 地址比较少的情况，使用公网地址池（202.169.10.80～202.169.10.83），采用 IP 地址和端口的替换方式替换 B 区内部的主机地址（网段为 10.0.0.0/24），访问 Internet。

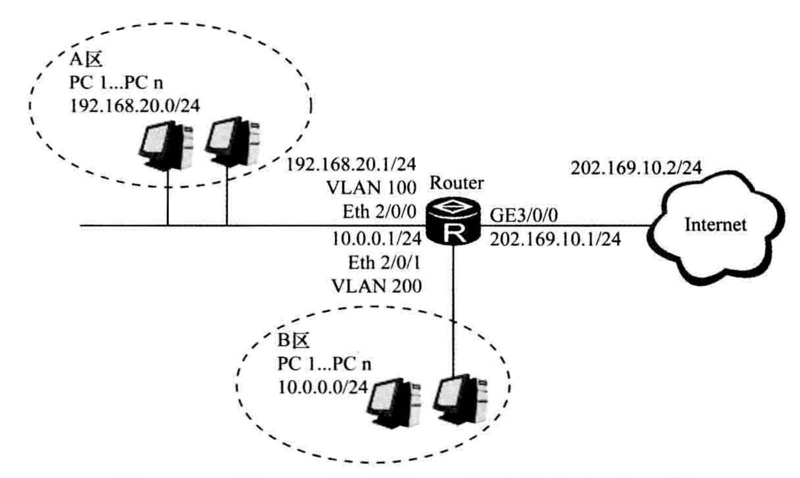


图 6-15　动态 NAT 地址转换配置示例的基本网络结构

1. 基本配置思路分析

本示例中有两个不同的内网用户区域，采用了不同的公网地址池，且是多对一的 NAT 地址转换（因为同时上网的内网用户可能多于地址池中的公网地址数，如果确定不会多于公网地址数，也可以用 Basic NAT），所以需要配置两个 NAT 地址池。然后通过两个 ACL 限制两个用户区域中允许使用对应动态地址转换应用的内部网络用户（当然，还需要在 NAT 设备上配置到达 Internet 的缺省路由）。

因本示例中没有 ALG、DNS Mapping、NAT 过滤和映射、NAT 日志输出、NAT 地址映射表项老化时间的应用需求，所以不进行这些方面的配置。

2. 具体配置步骤

① 配置 NAT 设备各接口 IP 地址。

因为 NAT 设备的内、外部接口均只能在三层模式下配置，所以首先需要配置好 NAT 设备上的内、外部接口 IP 地址。根据图中标注，内部 LAN 接口需要通过加入到对应的 VLAN 中，再在对应的 VLANIF 接口下配置 IP 地址，外部 WAN 接口可直接配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 100
[Router-vlan100] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 192.168.20.1 24
[Router-Vlanif100] quit
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access  !---因为该接口连接的是单个 VLAN，所以仅需要配置为不带标签的
Access，或者不带标签的 Hybrid 类型接口即可。下面的 Ethernet 2/0/1 的接口类型配置一样
[Router-Ethernet2/0/0] port default vlan 100
[Router-Ethernet2/0/0] quit
[Router] vlan 200
[Router-vlan200] quit
[Router] interface vlanif 200
[Router-Vlanif200] ip address 10.0.0.1 24
[Router-Vlanif200] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 200
```

```
[Router-Ethernet2/0/1] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 202.169.10.1 24
[Router-GigabitEthernet3/0/0] quit
```

② 配置两个用于控制 A 区和 B 区用户应用动态 NAT 地址转换的 ACL。因为这里仅需要控制作为源 IP 地址（不用控制通信协议类型）的用户私网 IP 地址，所以仅需配置基本 ACL 即可。

```
[Router] acl 2000
[Router-acl-basic-2000] rule 5 permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2000] quit
[Router] acl 2001
[Router-acl-basic-2001] rule 5 permit source 10.0.0.0 0.0.0.255
[Router-acl-basic-2001] quit
```

③ 配置两个动态 NAT 出接口地址关联。这里采用地址池的方式配置。

```
[Router] nat address-group 1 202.169.10.100 202.169.10.200
[Router] nat address-group 2 202.169.10.80 202.169.10.83
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] nat outbound 2000 address-group 1
[Router-GigabitEthernet3/0/0] nat outbound 2001 address-group 2
[Router-GigabitEthernet3/0/0] quit
```

④ 配置到达 Internet 的缺省路由，指定下一跳地址为运营商侧设备 IP 地址 202.169.10.2。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

说明 如果需要在 Router 上执行 **ping-a** *source-ip-address* 命令，通过指定发送 ICMP ECHO-REQUEST 报文的源 IP 地址来验证内网用户是否可以访问 Internet，则还需要配置 **ip soft-forward enhance enable** 命令，使能设备产生的控制报文的增强转发功能，这样 ping 报文中的私网源 IP 地址才能通过 NAT 转换为公网地址，使得最终的 ICMP 回应报文正确返回私网 ping 主机上。

配置好后，可以在 Router 上执行 **display nat outbound** 命令，查看地址转换配置，具体如下。

```
<Router> display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------
 Interface              Acl      Address-group/IP/Interface    Type
 --------------------------------------------------------------
 GigabitEthernet3/0/0   2000                   1                pat
 GigabitEthernet3/0/0   2001                   2                pat
 --------------------------------------------------------------
   Total : 2
```

6.3.9 配置两次 NAT 示例

本示例的基本拓扑结构如图 6-16 所示，路由器出接口 GE1/0/0 的 IP 地址为 202.11.1.2/24，LAN 侧接口 IP 地址为 202.10.0.1/24，对端运营商 IP 地址为 202.11.1.1/24。公司内网一台主机的 IP 地址分配不合理，PC-1 和公网中的服务器 Server A 的地址重叠。这时，内部网络主机 PC-2 使用 Server A 的域名访问该服务器时很可能访问到的是同一内网中的主机 PC-1，自然就不能满足要求了。现用户希望通过两次 NAT 的方案解决。

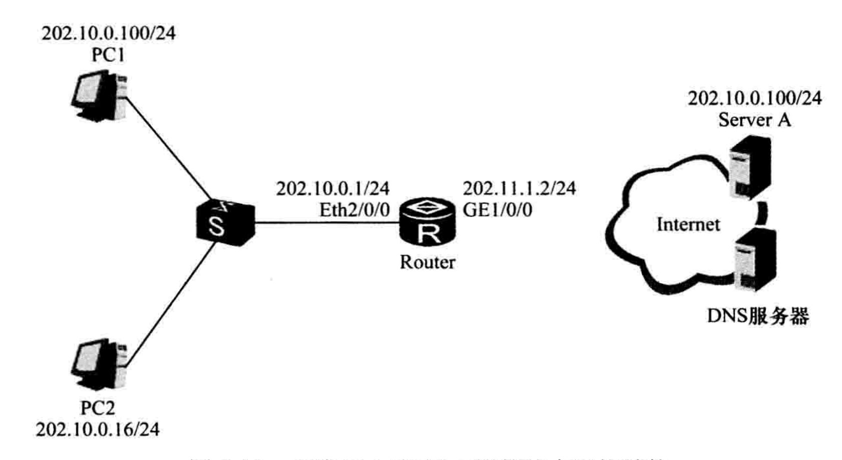


图 6-16　两次 NAT 配置示例的基本网络结构

1. 基本配置思路分析

首先要明确，这是一个通过动态 NAT 实现内网主机访问外网主机的示例，但本示例有一个特殊之处就是在内网中有一个主机的 IP 地址与内网用户要访问的外网服务器主机的 IP 地址相同，造成了 IP 地址重叠，所以本示例在需要配置动态 NAT 的情况下还要配置两次 NAT。在配置动态 NAT 时，地址池为临时地址池，然后通过两次 NAT 配置临时地址池与重叠的公网地址池之间的映射关系（**临时地址池与重叠地址池要处于不同的 IP 网段**）。另外，因为 PC2 主机使用的是域名访问方式，所以本示例还需要同时配置 DNS ALG（但不需要配置 DNS Mapping，因为 DNS Mapping 仅用于从外网访问内网服务器的 NAT Server 实现方式中）。

2. 具体配置步骤

① 配置各接口的 IP 地址。从图中标注可以看出，这里 LAN 接口和 WAN 接口均为三层接口，可直接配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 202.11.1.2 24
[Router-GigabitEthernet1/0/0] quit
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] ip address 202.10.0.1 24
[Router-Ethernet2/0/0] quit
```

② 配置两次 NAT。两次 NAT 主要是配置重叠的公网地址池到临时地址池之间的映射关系（假设临时地址池的起始地址为 202.12.1.100，共 254 个），还需要配置从出接口 GE1/0/0 到达临时地址的静态路由。

```
[Router] nat overlap-address 0 202.10.0.100 202.12.1.100 pool-length 254
[Router] ip route-static 202.12.1.100 32 gigabitethernet 1/0/0 202.11.1.1
```

③ 配置动态 NAT。

```
[Router] acl 3180
[Router-acl-adv-3180] rule 5 permit ip source 202.10.0.0 0.0.0.255   !---定义允许内部地址使用 NAT 地址转换的高级
ACL 规则（同时限定仅允许 IP 通信可使用 NAT 地址转换）
[Router-acl-adv-3180] quit
[Router] nat address-group 1 202.11.1.100 202.11.1.200
[Router] interface gigabitethernet 1/0/0
```

```
[Router-GigabitEthernet1/0/0] nat outbound 3180 address-group 1   !---在NAT出接口上关联内部网络地址和NAT公网地址池
[Router-GigabitEthernet1/0/0] quit
[Router] nat alg dns enable   !---使能DNS的NAT ALG功能
```

④ 配置到达 Internet 的缺省路由，指定下一跳地址为 202.11.1.1。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.11.1.1
```

配置好后，可执行 **display nat overlap-address all** 命令查看地址池映射关系。具体如下。

```
<Router> display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:
 ---------------------------------------------------------------------------
 Id   Overlap-Address    Temp-Address      Pool-Length          Inside-VPN-Instance-Name
 ---------------------------------------------------------------------------
 0    202.10.0.100       202.12.1.100      254
 ---------------------------------------------------------------------------
   Total : 1
```

也可执行 **display nat outbound** 命令查看 NAT 地址池信息。具体如下。

```
[Router] display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------
 Interface                  Acl        Address-group/IP/Interface        Type
 ----------------------------------------------------------------
 GigabitEthernet1/0/0       3180                          1                 pat
 ----------------------------------------------------------------
   Total : 1
```

6.4 配置静态 NAT

静态 NAT 可以实现私网 IP 地址和公网 IP 地址的固定一对一映射，其基本的配置思想就是配置用户私网 IP 地址与用于 NAT 地址转换的公网 IP 地址之间的一对一静态映射表项。同时，也可根据实际需要选择配置在 6.2 节介绍的其他 NAT 扩展应用技术，具体可配置的任务如下（**仅第一项为必选配置任务**）。各可选配置任务之间没有严格的先后配置次序。因为后面 5 项可选配置任务均已在 6.3 节中有对应的介绍，且配置方法完全一样，故在此不再赘述。

① 配置静态地址映射。

②（可选）配置 DNS Mapping。

③（可选）使能 NAT ALG 功能。

这项配置任务与 6.3.3 小节介绍的配置方法完全一样，参见即可。

④（可选）配置 NAT 过滤方式和映射模式。

这项配置任务与 6.3.4 小节介绍的配置方法完全一样，参见即可。

⑤（可选）配置两次 NAT。

这项配置任务与 6.3.5 小节介绍的配置方法完全一样，参见即可。

⑥（可选）配置 NAT 日志输出。

这项配置任务与 6.3.6 小节介绍的配置方法完全一样，参见即可。

⑦（可选）配置 NAT 地址映射表项老化时间。

这项配置任务与 6.3.7 小节介绍的配置方法完全一样，参见即可。

6.4.1　配置静态 NAT 地址映射

配置静态地址映射就是配置私网 IP 地址与公网 IP 地址的一对一映射表项，可以在系统视图下为所有 NAT 出口全局配置，也可以在 NAT 出接口视图下仅为该接口配置。

在系统视图配置 NAT 静态映射的步骤如表 6-5 所示。在接口视图下配置 NAT 静态映射的步骤如表 6-6 所示。

表 6-5　　在系统视图下全局配置静态 NAT 映射的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**nat static protocol** { **tcp** | **udp** } **global** *global-address global-port* **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*] 或 **nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*] 或 **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*] 例如：[Huawei] **nat static protocol tcp global interface loopback** 4 43 **inside** 192.168.2.55 **netmask** 255.255.255.255 （在 TCP 报文中，以公网地址为 Loopback 4 接口 IP 地址，端口为 43，与对应的私网地址 192.168.2.55 之间建立对应转换关系） 或 [Huawei] **nat static protocol tcp global** 1.1.1.1 43 **inside** 192.168.2.2 **netmask** 255.255.255.0 （在 TCP 报文中，以公网 IP 地址 1.1.1.1（24 位掩码）网段，端口为 43，与对应的私网 IP 地址 192.168.2.2（24 位掩码）网段之间建立对应转换关系，**即所有与 192.168.2.2/24 在同一网段的私网 IP 地址都将一一对应转换为 1.1.1.1/24 所在网段中的 IP 地址**）	（三选一）配置从私网 IP 地址到公网 IP 地址的一对一映射。三个命令中的参数和选项说明如下 • *protocol-number*：指定地址映射所作用的通信协议的协议号，取值范围为 1～255 的整数。仅当所应用的通信协议类型不是 ICMP、TCP 和 UDP 时才需要指定 • **icmp** | **tcp** | **udp**：指定所配置的 NAT 地址映射所作用的通信协议分别为 ICMP 协议、TCP 协议，或者 UDP 协议 • *global-address*：指定 NAT 地址映射表项中的公网 IP 地址 • *host-address*：指定 NAT 地址映射表项中的私网 IP 地址 • *global-port*：指定 NAT 地址映射表项中提供给外部访问的服务的端口号，取值范围为 0～65 535 的整数。如果不配置此参数，则表示端口号为零，即任何类型的服务都提供 • *host-port*：可选参数，指定 NAT 地址映射表项中内部主机提供的服务端口号，取值范围为 0～65 535 的整数。如果不配置此参数，则和 *global-port* 参数值所指定的端口号一致 • **vpn-instance** *vpn-instance-name*：指定 NAT 地址映射作用的 VPN 实例的名称，1～31 个字符 • **netmask** *mask*：可选参数，指定静态 NAT 网络掩码，取值范围为 255.255.255.0～255.255.255.255，即最多 255。但注意，**这里不是映射地址中的子网掩码**，仅用来指定可建立的地址映射表项数（最多为 255 个），如果仅一个 IP 地址之间的映射，则静态 NAT 网络掩码为 255.255.255.255，如果是一个子网（**一定是 24 位子网掩码**）的全部映射，则静态 NAT 网络掩码为 255.255.255.0。缺省为 255.255.255.255，即单个 IP 地地址之间的映射 • **description** description：可选参数，指定 NAT 地址映射的描述信息，1～255 个字符，支持空格，区分大小写，字符串中不能包含“?” • **interface loopback** *interface-number*：指定公网 IP 地址为对应编号的 Loopback 的接口 IP 地址，取值范围为 0～1 023 的整数 缺省情况下，系统未配置私网 IP 地址到公网 IP 地址的一对一转换，这三个命令分别可用对应的 **undo** 格式命令删除全局下已经配置的指定静态 NAT 地址一对一转换

（续表）

步骤	命令	说明
3	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 NAT 出接口（必须是三层接口，但不能是 Loopback 接口和 NULL 接口），进入接口视图
4	**nat static enable** 例如：[Huawei-GigabitEthernet1/0/0] **nat static enable**	在以上 NAT 出接口下使能 NAT 静态地址映射功能 缺省情况下，接口未使能 NAT 静态地址映射功能，可用 **undo nat static enable** 命令用来去使能接口下的 NAT 静态地址映射功能

表 6-6　在接口视图下配置 NAT 静态映射的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 NAT 出接口（必须是三层接口，但不能是 Loopback 接口和 NULL 接口），进入接口视图
3	**nat static protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** } *global-port* **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*] 或 **nat static protocol** { **tcp** | **udp** } **global interface** *interface-type interface-number global-port* [**vpn-instance** *vpn-instance-name*] **inside***host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*] 或 **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*] 例如：[Huawei-GigabitEthernet1/0/0] **nat static protocol tcp global** 202.10.10.1 200 **inside** 10.10.10.1 300 （在 TCP 报文中，以公网地址为 202.10.10.1，端口为 200 与对应的私网地址是 10.10.10.1，端口为 300 之间建立对应转换关系） 或 [Huawei-GigabitEthernet1/0/0] **nat static global** 3.3.3.3 **inside** 2.2.2.2 **vpn-instance huawei netmask** 255.255.255.0 （将来自 VPN 为 huawei 并且与 IP 地址 2.2.2.2（24 位掩码）在同一网段的报文，替换为 3.3.3.3（24 位掩码）网段的对应 IP 地址）	（三选一）配置从私网 IP 地址到公网 IP 地址的一对一映射。三个命令中除以下参数和选项外，其他参数和选项说明参见表 6-5 中的第 2 步 ● **acl** *acl-number*：可选参数，指定控制在出接口下应用 NAT 静态地址转换的 NAT 应用的 ACL 编号，可以是基本 ALC 或者高级 ACL，取值范围为 2 000～3 999 ● **current-interface**：二选一选项，指定以当前接口 IP 地址作为公网 IP 地址 ● **interface** *interface-type interface-number*：指定以指定接口 IP 地址作为公网 IP 地址 缺省情况下，系统未配置私网 IP 地址到公网 IP 地址的一对一转换，这三个命令分别可用以下命令删除在接口下已经配置的指定静态 NAT 地址一对一转换 ● **undo nat static protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** } *global-port* **inside** *host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] ● **undo nat static protocol** { **tcp** | **udp** } **global interface** *interface-type interface-number global-port* [**vpn-instance** *vpn-instance-name*] **inside***host-address* [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] ● **undo nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*]

注意　配置静态 NAT 时，其中的 *global-address* 和 *host-address* **必须保证和所有设备现有地址没有重复**，包括设备接口地址、用户地址池地址，以避免冲突。

在设备上执行 **undo nat static** 命令，设备上的静态映射表项不会立刻消失。如果需要立刻清除静态 NAT 映射表项，需手动执行 **reset nat session** 命令来清除静态映射表项信息。

在多个接口使用同一条 **nat staic** 命令配置的映射情况下，建议使用在系统视图下配置的方法。

当配置借用接口地址的静态 1:1 NAT（不指定端口号，接口地址对应一个私网地址）时，可能会造成在该接口地址上启用的其他业务无法正常使用，需谨慎选择，如果确定在该接口地址上启用其他应用，请在配置后面增加 ACL 排除启用应用的端口号。

6.4.2　配置 DNS Mapping

内网用户可以通过 NAT 使用外网的 DNS 服务器访问外网的服务器，但如果内网用户通过外网的 DNS 服务器访问内网服务器时就会失败。因为来自外网的 DNS 解析结果是内网服务器对外宣称的公网 IP 地址，并非内网服务器真实的私网 IP 地址。所以，**如果没有内网的 DNS 服务器，而且又有使用域名访问内网服务器的需求**，这就要求企业内网用户必须使用外网的 DNS 服务器来实现域名访问，这时就得配置 DNS Mapping 功能。

在配置静态地址转换时配置 DNS Mapping，可以指明“域名-公网 IP 地址-公网端口-协议类型”映射表项。当 DNS 解析报文到达 NAT 设备时，NAT 设备会根据 DNS Mapping 建立的映射表项中的公网域名对应的公网 IP 地址查找静态地址表项，得到公网 IP 地址对应的私网 IP 地址，再用该私网地址替换 DNS 的解析报文数据部分的内部服务器公网 IP 地址并转发给用户。**但 DNS 报文必须与 NAT ALG 结合使用，否则仍不能正常穿越 NAT**。具体的配置步骤如表 6-7 所示。

表 6-7　DNS Mapping 的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**nat dns-map** *domain-name global-address global-port* { **tcp** | **udp** } 例如：[Huawei]**nat dns-map** www.test.com 20.1.1.1 2012 **tcp**	配置域名到公网 IP 地址、端口号、协议类型的映射。命令中的参数和选项说明如下 • *domain-name*：指定可被公网 DNS 服务器正确解析的合法域名，也就是内部服务器的域名 • *global-address*：指定内部服务器提供给公网访问的公网 IP 地址 • *global-por*：指定内部服务器提供给公网访问的服务端口号，取值范围为 1～65 535 的整数 • **tcp** | **udp**：指定进行的网络应用所使用的传输层通信协议类型 缺省情况下，系统未配置域名到公网 IP 地址、端口号、协议类型的映射，可用 **undo nat dns-map** *domain-name* 命令删除一条域名到公网 IP 地址、端口号、协议类型的映射

（续表）

步骤	命令	说明
3	**nat alg dns enable** 例如：[Huawei]**nat alg dns enable**	（可选）使能 DNS ALG 功能，使 DNS 应答报文正常穿越 NAT，否则内部主机无法使用域名访问内网服务器 **如果已配置了 NAT DNS ALG 任务，则无需再重复配置本命令** 缺省情况下，NAT DNS ALG 处于未使能状态，可用 **undo nat alg dns enable** 命令关闭 NAT DNS ALG 功能

6.4.3 静态一对一 NAT 配置示例

本示例的基本拓扑结构如图 6-17 所示，路由器的出接口 GE2/0/0 的 IP 地址为 202.10.1.2/24，LAN 侧网关地址为 192.168.0.1/24。对端运营商侧地址为 202.10.1.1/24。现 IP 地址为 192.168.0.2/24 的内网主机需要使用固定的公网 IP 地址 202.10.1.3/24 来访问 Internet。

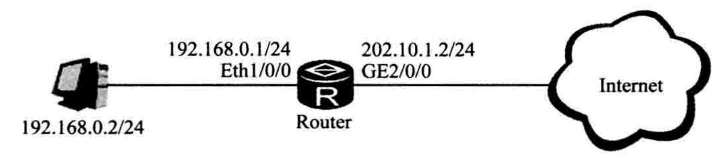


图 6-17 一对一静态 NAT 配置示例的基本网络结构

1. 基本配置思路分析

这是一个仅要求配置一条一对一的静态 NAT 地址转换的配置示例。根据 6.4.1 小节介绍的配置方法，可以知道最基本的配置就是要求在系统视图或者出接口视图下配置静态地址转换表（当然，同样需要在 NAT 设备上配置到达 Internet 的缺省路由），其他可选配置任务本示例均可不配置，因为没有这方面的实际应用需求。

2. 具体的配置步骤

① 配置各接口 IP 地址。根据图中标注，本示例中的 LAN 和 WAN 接口都是三层接口，均可直接配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 202.10.1.2 24
[Router-GigabitEthernet2/0/0] quit
[Router] interface ethernet 1/0/0
[Router-Ethernet1/0/0] ip address 192.168.0.1 24
[Router-Ethernet1/0/0] quit
```

② 配置出接口 GE2/0/0 一对一的静态 NAT 映射表项。

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] nat static global 202.10.1.3 inside 192.168.0.2
[Router-GigabitEthernet2/0/0] quit
```

③ 配置到达 Internet 的缺省路由，下一跳地址为运营商侧 IP 地址 202.10.1.1。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.10.1.1
```

配置好后，可在 Router 上执行 **display nat static** 命令查看地址池映射关系。具体如下。

```
<Router> display nat static
  Static Nat Information:
  Interface    : GigabitEthernet2/0/0
    Global IP/Port         : 202.10.1.3/----
    Inside IP/Port         : 192.168.0.2/----
    Protocol : ----
    VPN instance-name    : ----
    Acl number              : ----
    Netmask    : 255.255.255.255
    Description : ----

  Total :      1
```

6.5　配置 NAT Server

NAT Server 功能是为了解决外网用户访问采用私网 IP 地址的内网服务器的一种 NAT 方案（前面所说的动态 NAT 和静态 NAT 都是针对内网访问外网的情形），所以又称为“内部服务器”NAT 方案。

NAT Server 的基本配置思想就是为内部服务器创建全局公网 IP 地址到内部私网 IP 地址之间的一对一静态映射表项，同样还可根据实际需要选择配置 6.2 节介绍的其他 NAT 扩展应用技术，具体可配置的任务如下（**仅有第一项是必选的**）。可选配置任务的配置方法与前面 6.3 节和 6.4 节中对应配置任务中的完全一样，参见即可。

（1）配置内部服务器地址映射

（2）（可选）配置 DNS Mapping

这项配置任务与 6.4.2 小节介绍的配置方法完全一样，参见即可。

（3）（可选）使能 NAT ALG 功能

这项配置任务与 6.3.3 小节介绍的配置方法完全一样，参见即可。

（4）（可选）配置 NAT 过滤方式和映射模式

这项配置任务与 6.3.4 小节介绍的配置方法完全一样，参见即可。

（5）（可选）配置两次 NAT

这项配置任务与 6.3.5 小节介绍的配置方法完全一样，参见即可。

（6）（可选）配置 NAT 日志输出

这项配置任务与 6.3.6 小节介绍的配置方法完全一样，参见即可。

（7）（可选）配置 NAT 地址映射表项老化时间

这项配置任务与 6.3.7 小节介绍的配置方法完全一样，参见即可。

6.5.1　配置 NAT Server 地址映射

在 NAT Server 中，也要像静态 NAT 那样配置 NAT 地址转换映射表，用来一对一地配置内部服务器的地址映射表项，具体配置步骤如表 6-8 所示。

表 6-8 内部服务器地址映射的配置步骤

<table>
<tr><th>步骤</th><th>命令</th><th>说明</th></tr>
<tr><td>1</td><td>system-view
例如：< Huawei > system-view</td><td>进入系统视图</td></tr>
<tr><td>2</td><td>interface interface-type interface-number
例如：[Huawei] interface gigabitethernet 1/0/0</td><td>键入外网主机访问内部服务器的接口（不一定是 NAT 出接口，但必须是三层接口，但不能是 Loopback 接口和 NULL 接口），进入接口视图</td></tr>
<tr><td rowspan="3">3</td><td>nat server protocol { tcp | udp } global { global-address | current-interface } global-port inside host-address [host-port] [vpn-instancevpn-instance-name] [acl acl-number] [description description]</td><td rowspan="3">（三选一）定义一个内部服务器的映射表，外部用户可以通过地址和端口转换来访问内部服务器的某项服务。命令中的参数和选项说明如下
● icmp | tcp | udp：指定应用内部服务器地址映射的通信协议类型（ICM、TCP 或者 UDP）
● protocol-number：指定本内部服务器地址映射所应用的通信协议索引号，取值范围为 1～255 的整数
● global-address：多选一参数，内部服务器提供给外部网络访问的公网 IP 地址
● current-interface：多选一选项，指定当前 NAT 出接口 IP 地址为内部服务器的公网 IP 地址
● interface interface-type interface-number：多选一参数，指定以指定接口的 IP 地址作为内部服务器的公网 IP 地址
● global-port：内部服务器提供给外部网络访问的公网端口号（要对应前面的通信协议类型的选择）。常用的端口号可以用关键字代替，例如 FTP 服务端口号为 21，同时可以使用 ftp 代替。如果不配置此参数，则表示是 any 的情况，即端口号为零，可以提供任何类型的服务
● host-address：内部服务器的私网 IP 地址
● host-port：可选参数，内部服务器的私网端口号（要对应前面的通信协议类型的选择）
● acl acl-number：可选参数，指定控制在出接口下应用内部服务器地址映射表的 NAT 应用的 ACL 编号，可以是基本 ACL 或者高级 ACL，取值范围为 2 000～3 999
● description description：为本内部服务器地址映射配置描述信息，1～255 个字符，支持空格，区分大小写，字符串中不能包含“?”
缺省情况下，系统未配置私网 IP 地址到公网 IP 地址的一对一转换，这三个命令分别可用以下对应的命令删除对应的内部服务器映射表
● undo nat server protocol { tcp | udp } global { global-address | current-interface } global-port inside host-address [host-port] [vpn-instance vpn-instance-name]
● undo nat server protocol { tcp | udp } global interface interface-type interface-number global-port [vpn-instance vpn-instance-name] insidehost-address [host-port] [vpn-instance vpn-instance-name]
● undo nat server [protocol { protocol-number | icmp | tcp | udp }] global { global-address | current-interface | interface interface-type interface-number } inside host-address [vpn-instance vpn-instance-name]</td></tr>
<tr><td>nat server protocol { tcp | udp } global interface interface-type interface-number global-port [vpn-instance vpn-instance-name] inside host-address [host-port] [vpn-instance vpn-instance-name] [acl acl-number] [description description]</td></tr>
<tr><td>nat server [protocol { protocol-number | icmp | tcp | udp }] global { global-address | current-interface | interface interface-type interface-number } inside host-address [vpn-instance vpn-instance-name] [acl acl-number] [description description]
例如：[Huawei-GigabitEthernet1/0/0]nat server protocol tcp global 143.242.14.79 inside 192.168.0.1（添加一个内部服务器地址映射表，将 TCP 协议的公网 143.242.14.79 地址转换为内网的 192.168.0.1）</td></tr>
</table>

注意 在上表第3步的配置 NAT Server 地址映射的命令中，参数 *global-address* 和 *host-address* **必须保证和所有设备上现有地址没有重复**，包括设备接口地址、用户地址池地址等，以避免冲突。

如果使用接口地址作为内网服务器地址，可以使用 **current-interface**，也可以指定实际存在的 **loopback** 接口地址作为内网服务器地址。

在设备上执行 **undo nat server** 命令，设备上的映射表项不会立刻消失，需要手动执行 **reset nat session** 命令来清除表项信息。

NAT Server 和静态 NAT 的区别就是 NAT Server 对于内网主动访问外网的情况不做端口替换，仅做地址替换，因为 Internet 中这些服务都是直接使用其对应的默认端口，不可更改。

当配置借用接口地址的 1:1 NAT Server（不指定端口号，接口地址对应一个私网地址）时，可能会造成在该接口地址上启用的其他业务无法正常使用，请谨慎选择。如果确定在该接口地址上启用其他应用，请在配置后面增加 ACL 排除启用应用的端口号。

【经验之谈】在 NAT Server 的配置中往往涉及一个内网用户访问内部服务器的需求问题，而且有些情形下还可能造成内网用户不能访问配置了。下面列举这些内网用户访问通过 NAT 映射了公网 IP 地址的内部服务器的情形以及它们所需的配置。

① 当内网服务器**有域名，DNS 服务器在内网侧，内网用户需要通过域名访问**内部服务器，或者内网服务器**没有域名，内网用户需要通过私网 IP 地址访问**内部服务器时，无需另外的配置，只需在 NAT 设备上配置好内部服务器地址映射就可以了。

② 当内网服务器**有域名，DNS 服务器在公网侧，内网用户需要通过域名访问**内部服务器，这时除了需要配置内部服务器地址映射外，还需要配置 DNS Mapping 和 DNS ALG。

③ 内网服务器**没有域名，内网用户通过公网 IP 地址访问**内部服务器，这时除了需要配置内部服务器地址映射外，还需要通过 QoS 流策略重定向下一跳行为，定义内部网络用户以公网 IP 地址访问内部服务器时的下一跳为 NAT 出接口 IP 地址，并在 NAT 内部接口方向进行应用。下面是一个流策略重定向的示例，假设内部网络的 IP 网段为 192.168.1.0/24，内部服务器的公网 IP 地址为 1.1.1.10/24，NAT 出接口 IP 地址为 1.1.1.1/24，NAT 内部接口为 Ethernet 0/0/1。有关 QoS 流策略的创建与配置方法请参见配套图书《华为交换机学习指南》第 11 章。

```
<Huawei> system-view
[Huawei]acl number 3000
[Huawei-acl-adv-3000]rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.10 0
                                              !---定义一个由内部网络访问内部服务器公网 IP 地址的高级 ACL
[Huawei-acl-adv-3000]quit
[Huawei]traffic classifier redirect operator or          !---创建流分类，并指明下面的匹配规划为逻辑或类型
[Huawei-classifier- redirect]if-match acl 3000
[Huawei-classifier- redirect]quit
[Huawei]traffic behavior redirect                        !---创建流行为
[Huawei-behavior- redirect] redirect ip-nexthop 1.1.1.1  !----重定向下一跳为 NAT 出接口 IP 地址
[Huawei-behavior- redirect]quit
```

```
[Huawei]traffic policy redirect                                   !---创建流策略
[Huawei-trafficpolicy-redirec] classifier redirect behavior redirect   !---关联流分类和流行为
[Huawei-trafficpolicy-redirec]quit
[Huawei]interface Ethernet0/0/1
[Huawei-Ethernet0/0/1] traffic-policy redirect inbound------------在NAT内部接口入方向上应用以上流策略
```

6.5.2 NAT Server 地址映射配置示例

本示例的基本拓扑结构如图 6-18 所示，某公司的网络提供 WWW Server 和 FTP Server 供外部网络用户访问。WWW Server 的内部 IP 地址为 192.168.20.2/24，提供服务的端口为 8080，对外公布的地址为 202.169.10.5/24。FTP Server 的内部 IP 地址为 10.0.0.3/24，对外公布的地址为 202.169.10.33/24，对端运营商侧地址为 202.169.10.2/24。要求通过路由器的 NAT 功能把该公司的内部网络连接到 Internet 上。

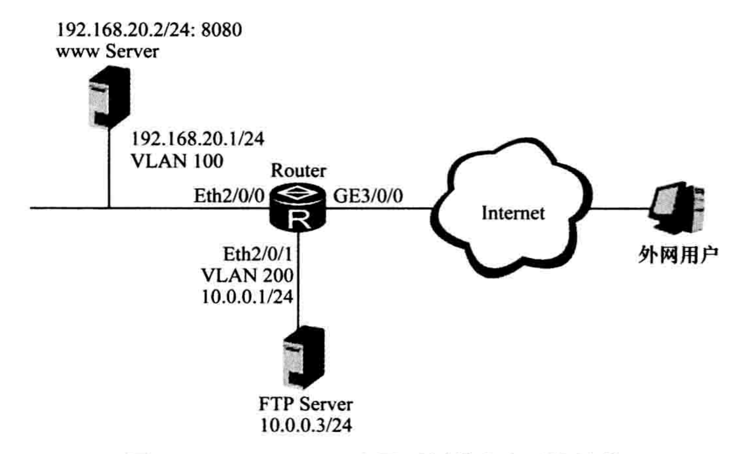


图 6-18 NAT Server 配置示例的基本网络结构

1. 基本配置思路分析

本示例的要求比较简单，仅要求把内部 WWW 服务器、FTP 服务器发布到 Internet 上，而没有要求采用域名访问 WWW 服务器（即不需要 DNS 服务），也没要求内网用户能通过服务器的公网 IP 地址或域名访问，所以仅需要配置基本的 NAT Server 即可，不需要配置 DNS Mapping 和流策略重定向。对于 WWW 服务器也就不需要配置 DNS ALG，但对于 FTP 服务器，仍需要配置 ALG FTP。

2. 具体配置步骤

① 配置各接口 IP 地址。这里假设连接 WWW 和 FTP 服务器的两 LAN 接口是二层接口，都必须先加入到一个 VLAN 中，然后在对应的 VLANIF 接口上配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 100
[Router-vlan100] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 192.168.20.1 24
[Router-Vlanif100] quit
```

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 100
[Router-Ethernet2/0/0] quit
[Router] vlan 200
[Router-vlan200] quit
[Router] interface vlanif 200
[Router-Vlanif200] ip address 10.0.0.1 24
[Router-Vlanif200] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 200
[Router-Ethernet2/0/1] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 202.169.10.1 24
```

② 配置 WWW 和 FTP 服务器地址映射。

```
[Router-GigabitEthernet3/0/0] nat server protocol tcp global 202.169.10.5 www inside 192.168.20.2 8080
[Router-GigabitEthernet3/0/0] nat server protocol tcp global 202.169.10.33 ftp inside 10.0.0.3 ftp
[Router-GigabitEthernet3/0/0] quit
```

③ 使能 FTP 的 NAT ALG 功能。

```
[Router] nat alg ftp enable
```

④ 配置到达 Internet 的缺省路由，下一跳地址为运营商侧的 IP 地址 202.169.10.2。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

配置好后，可以执行 **display nat server** 命令检查 NAT Server 配置，验证配置结果。具体如下。

```
<Router> display nat server
  Nat Server Information:
 Interface   : gigabitethernet 3/0/0
   Global IP/Port        : 202.169.10.5/80(www)
   Inside IP/Port        : 192.168.20.2/8080
   Protocol : 6(tcp)
   VPN instance-name     : ----
   Acl number            : ----
   Description           : ----

   Global IP/Port        : 202.169.10.33/21(ftp)
   Inside IP/Port        : 10.0.0.3/21(ftp)
   Protocol : 6(tcp)
   VPN instance-name     : ----
   Acl number            : ----
   Description           : ----

 Total :     2
```

6.5.3 NAT 综合配置示例

本示例的基本网络结构如图 6-19 所示，Web 服务器的内部 IP 地址为 192.168.0.100/24，采用 8080 端口提供 Web 服务；对外发布的公网 IP 地址为 202.10.1.3/24，域名为 www.TestNat.com。NAT 路由器出接口 GE1/0/0 的 IP 地址为 202.10.1.2/24，内部接口 Eth2/0/0 的 IP 地址为 192.168.0.1。除此之外，该公司没有其他公网 IP 地址。对端运营商侧地址为 202.10.1.1/24。现该公司要求通过公司内部的 Web 服务器对外网用户提供 Web

服务，同时公司的内网用户还可以访问外网，而且内网用户也可以通过外网的 DNS 服务器使用域名访问公司内部的 Web 服务器。

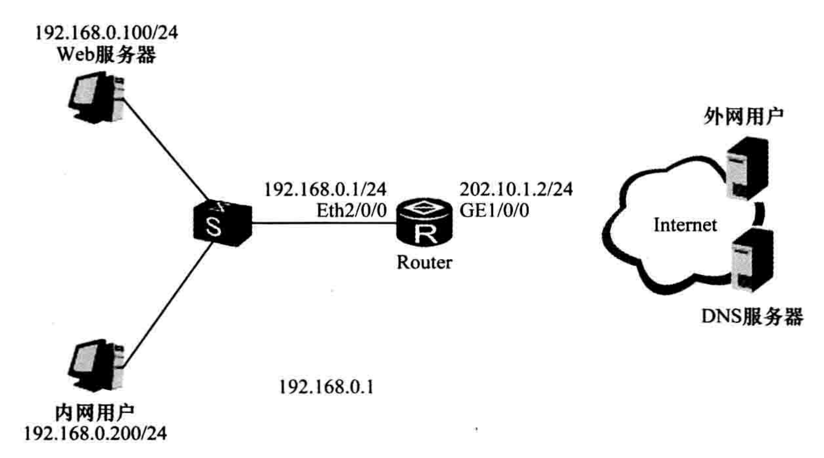


图 6-19 NAT 综合配置示例的基本网络结构

1. 基本配置思路分析

本示例的条件和要求主要有以下几个方面。

① 仅有一个公网 IP 地址配置在 NAT 路由器的出接口上，所以无论是内部网络用户访问 Internet，还是访问在 Internet 中发布的内部 Web 服务器，都只能通过一个公网 IP 地址进行。内部网络用户访问 Internet 可以通过 Easy IP 来实现（以 NAT 路由器出接口 IP 地址作为动态映射的公网 IP 地址），而公网用户或者内部网络用户访问发布到了 Internet 中 Web 服务器，只能通过 NAT Server 来实现。所以本示例要同时配置 Easy IP 和 NAT Server。

② 用户要能够通过域名访问位于内部网络，且 DNS 服务器又位于 Internet 的 Web 服务器，这时就需要同时配置 DNS ALG 和 DNS Mapping。

2. 具体配置步骤

① 配置各接口 IP 地址。根据图中标注，LAN 和 WAN 接口都是三层接口，均可直接配置 IP 地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 202.10.1.2 24
[Router-GigabitEthernet1/0/0] quit
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] ip address 192.168.0.1 24
[Router-Ethernet2/0/0] quit
```

② 配置 Easy IP。

```
[Router] acl 2000
[Router-acl-basic-2000] rule 5 permit source 192.168.0.0 0.0.0.255   !---定义用于指定 NAT 内部网络用户地址的基本
ACL 规则
[Router-acl-basic-2000] quit
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] nat outbound 2000   !---在出接口上把内部网络地址与本接口 IP 地址进行关联
[Router-GigabitEthernet1/0/0] quit
```

③ 配置 NAT Server。

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] nat server protocol tcp global 202.10.1.3 www inside 192.168.0.100 8080  !---配置内部Web服务器公网IP地址、公网端口号（以www代表标准的80端口）和私网IP地址、私网端口号的映射
[Router-GigabitEthernet1/0/0] quit
```

④ 配置 DNS 的 NAT ALG 和 DNS Mapping 功能。

```
[Router] nat alg dns enable  !---使能DNS ALG功能
[Router] nat dns-map www.TestNat.com 202.10.1.3 80 tcp  !----配置内部Web服务器"域名-公网IP地址-端口号-协议类型"的映射表
[Router] quit
```

⑤ 配置到达 Internet 的缺省路由，指定下一跳地址为运营商侧公网 IP 地址 202.10.1.1。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.10.1.1
```

配置好后，可在 Router 上执行 **display nat outbound** 操作，查看 NAT 地址映射表，结果如下。从中可以看到，已在 NAT 出接口 GE1/0/0 上正确关联了内部 IP 地址（由 ACL 2000 指定）和公网 IP 地址。

```
<Router> display nat outbound
 NAT Outbound Information:
 -----------------------------------------------------------------
 Interface                  Acl      Address-group/IP/Interface      Type
 GigabitEthernet1/0/0       2000                      202.10.1.2      easyip
 --------------------------------------------------------------------------
  Total : 1
```

也可在 Router 上执行 **display nat server** 操作，查看 NAT Server 映射表，结果如下，从中可以看到已在 NAT 出接口 GE1/0/0 上正确配置了内部 Web 服务器的 NAT Server 映射表。

```
<Router> display nat server
  Nat Server Information:
  Interface   : GigabitEthernet 1/0/0
    Global IP/Port       : 202.10.1.3/80(www)
    Inside IP/Port       : 192.168.0.100 8080
    Protocol : 6(tcp)
    VPN instance-name    : ----
    Acl number           : ----
    Description : ----
  Total :     1
```

还可在 Router 上执行 **display nat alg** 操作，查看各协议的 ALG 功能使能情况，结果如下。从中可以看到只有 DNS 使能了 ALG 功能。

```
<Router> display nat alg
NAT Application Level Gateway Information:
----------------------------------
  Application              Status
----------------------------------
  dns                       Enabled
  ftp                      Disabled
  rtsp                     Disabled
  sip                      Disabled
----------------------------------
```

6.6 NAT 管理与故障排除

为了方便介绍，把以上各种 NAT 配置的管理放在本节一起介绍。本节同时还将介绍在 NAT 配置和应用中经常出现的三种典型故障的分析与排除方法。

6.6.1 NAT 管理

配置好以上各节配置的 NAT 配置后，可使用以下 **display** 任意视图命令查看相关 NAT 信息、监控 NAT 运行，验证配置结果，也可以使用以下用户视图命令清除相关 NAT 地址映射表项、NAT 会话或统计信息等。

① **display nat address-group** [*group-index*] [**verbose**]：查看指定或全部的 NAT 地址池的简要或者详细（选择 **verbose** 可选项时）配置信息。

② **display nat outbound** [**acl** *acl-number* | **address-group** *group-index* | **interface** *interface-type interface-number* [*.subnumber*]]：查看指定 ACL 或地址池或出接口下的 NAT 出接口地址关联信息。

③ **display nat static** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-typeinterface-name*]：查看公网地址或内网地址或出接口下的静态 NAT 配置信息。

④ **display nat server** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface***interface-type interface-number* | **acl** *acl-number*]：查看指定公网地址、内网地址或者出接口下的 NAT Server 地址映射表配置信息。

⑤ **display nat alg**：查看 NAT 地址转换中的 ALG 配置信息。

⑥ **display nat dns-map** [*domain-name*]：查看 DNS 映射信息。

⑦ **display nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }：查看 NAT 双向地址转换（也就是两次 NAT）的相关信息。

⑧ **display firewall-nat session aging-time**：查看 NAT 表项老化时间的相关信息。

⑨ **display nat filter-mode**：查看当前的 NAT 过滤方式。

⑩ **display nat mapping-mode**：查看 NAT 映射模式。

⑪ **display nat mapping table** { **all** | **number** }或者 **display nat mapping table inside-address** *ip-address* **protocol** { **tcp** |**udp** } **port** *port-number* [**vpn-instance** *vpn-instance-name*]：查看 NAT 映射表所有表项信息或个数。

⑫ **display nat session** { **all** [**verbose**] | **number** }或者 **display nat session** { [**protocol** { **icmp** | **tcp** | **udp** | *protocol-number* }] [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] } [**verbose**]：查看 NAT 的会话表信息。会话表创建是通过动态报文触发的，如果设备上没有动态报文，则没有任何会话表信息。

⑬ **reset nat session** { **all** | **transit interface** *interface-type interface-number* }：清除 NAT 会话信息。**nat alg**、**nat server**、**nat static**、**nat outbound** 等命令配置发生变化后，现有的报文链接并不会按新配置进行转发，如果需要使变化的配置立即生效，可执行本命令，以实现快速改变 NAT 配置。但该命令每 10 s 只能执行一遍。本命令可用于删除

所有的NAT会话表信息或删除某一个接口下的NAT会话表信息，命令执行时会给出提示Y或N，便于用户再次确认。

6.6.2　典型故障分析与排除

在NAT的配置和应用中，经常出现以下三种故障。

- 动态NAT中内网用户无法访问公网。
- NAT Server中外网主机无法访问内部服务器。
- 两次NAT中内网重叠地址主机无法访问内部服务器。

1. *动态NAT中内网用户无法访问公网*

这类故障的常见原因包括以下两个方面。

① 没有在NAT出接口上正确配置地址关联。

② 用于指定内部地址的ACL配置错误。

下面是具体的排除步骤。

① 在NAT设备上执行 **display interface** *interface-type interface-number*（这里为NAT内部接口）命令，查看显示信息的 **Input** 字段值，检查设备的接口是否有报文进入。

如果 **Input** 字段值为0，表示设备没有报文进入，请排查接口的配置，保证接口能接收报文；如果 **Input** 字段值不为0，请继续执行下一步。

② 在设备上执行 **display nat outbound** 命令，查看出接口上是否正确配置了NAT出接口关联。从显示信息可知NAT出接口关联的ACL号，然后查看对应ACL的规则配置是否正确。如果ACL未配置正确的IP地址、端口号或协议类型，将导致报文无法正常出入网络。

如果ACL匹配规则配置错误，请重新进行配置；如果ACL匹配规则配置正确，故障仍然存在，请继续执行下面的步骤。

③ 在设备上执行 **display nat address-group** 命令，查看出接口上所绑定的公网IP地址池是否正确。针对Easy IP方式，需要在设备上执行 **display nat outbound** 命令，查看NAT出接口上配置的Easy IP信息。

2. *NAT Server中外网主机无法访问内网服务器*

这类故障的常见原因主要包括两个方面。

① NAT Server配在错误的接口上（比如配置在出接口上，或其他不相关的接口上），正确应该配置在**外网主机访问内网的入接口上**。

② NAT Server配置错误（比如配置的内部Server对应的公网、私网IP地址不对，私网端口和内部服务器打开的端口不一样）。

下面是具体的排除步骤。

① 检查内网NAT Server上的应用服务正常。

当从外网无法访问 NAT Server 所提供的服务时，先确认内网服务器上相应的服务（例如HTTP Server，FTP Server等）是否打开。可以从内网其他主机上尝试访问内网服务器，以确保相应服务正在运行。

如果内网 NAT Server 上的应用服务未正常运行，请打开相应服务；如果内网 NAT

Server 上的应用服务正常运行，故障仍然存在，请继续执行下面的步骤。

② 在设备上执行 **display nat server** 命令，查看 NAT Server 是否配置在正确的 NAT 接口上，是否配置了正确的协议、端口和地址信息。

特别需要注意被映射的内网地址和端口是否正确。某些服务传送报文数据时，会使用到多个端口（有些端口是随机产生的），例如 FTP 和 TFTP，因此为这些服务配置 NAT Server 时，应该把对端口的限制放开，使得内部服务器可以正常提供服务。

如果 NAT Server 配置错误，请重新进行正确配置；如果 NAT Server 配置正确，故障仍然存在，请继续执行下面的步骤。

③ 检查 NAT Server 外网接口上的 IP 地址以及为 NAT Server 配置的公网 IP 地址是否正确。例如，是否和其他该网段的地址发生冲突。从外网主机上 ping NAT Server 的外网接口地址，确保外网主机到 NAT Server 之间的连通性。

如果外网主机和 NAT Server 外网接口之间的连通性存在问题，请检查并确保连通性正常；如果外网主机和 NAT Server 外网接口之间的连通性正常，故障仍然存在，请继续执行下面的步骤。

④ 检查内网服务器上是否配置了正确的路由或者网关，使得发向外网的报文可以正确地送到 NAT 网关。

3. 两次 NAT 中内网重叠主机无法访问外网服务器

本类故障的常见原因包括以下几个方面。

- 内网访问公网对应的出接口上配置 NAT 地址关联错误。
- 未使能 DNS 协议的 NAT ALG。
- 配置的 DNS Mapping 错误（比如，对应的公网地址和外网服务器 IP 地址不同）。
- 没有配置从内网临时地址到 NAT 公网出接口的路由。

下面是具体的排除步骤。

① 在设备上执行 **display nat outbound** 命令，查看 NAT 出接口上是否配置了地址关联。通过执行 **display nat address-group** 命令查看地址池配置信息。

最后再查看 NAT 出接口关联的 ACL 规则是否正确，ACL 规则常见问题有：没有配置合适的地址、协议、端口等，导致内网报文无法送出或外网报文无法进入。

如果 NAT 出接口地址关联配置错误，请修改对应配置；如果 NAT 出接口地址关联配置正确，故障仍然存在，请继续执行下面的步骤。

② 在设备上执行 **display nat dns-map** 命令，查看 DNS Mapping 是否配置在正确的 NAT 出接口上，是否配置了正确的协议、端口和地址信息。

如果 DNS Mapping 配置错误，请修改或重新配置；如果 DNS Mapping 配置正确，故障仍然存在，请继续执行下面的步骤。

③ 在设备上执行命令 **display nat alg**，查看 DNS ALG 是否使能。如果 DNS 的 NAT ALG 未使能，请使能；如果 DNS ALG 已使能，故障仍然存在，请继续执行下面的步骤。

④ 在设备上执行 **display nat overlap-address** 命令，查看所有已配置的重叠地址池

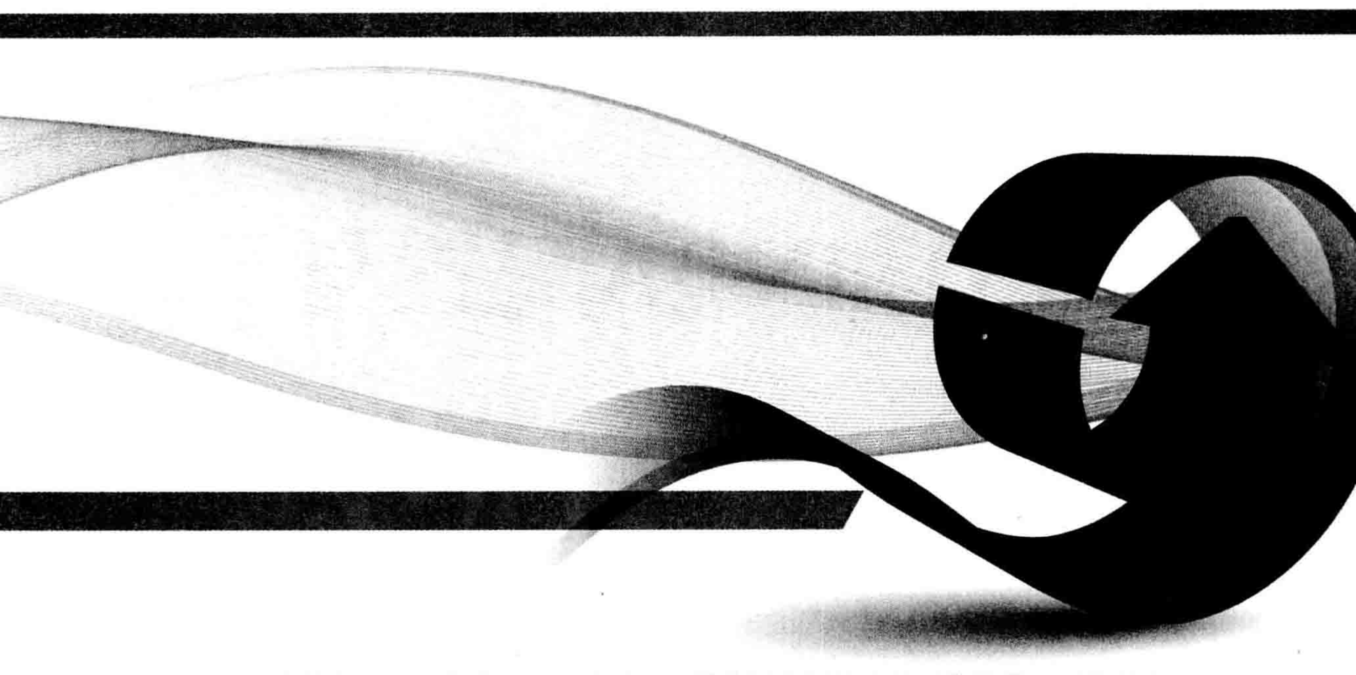
到临时地址池的映射是否正确。

临时地址池是设备上空闲可用的 IP 地址，不能和接口地址、VRRP 地址、NAT 类型地址存在冲突。如果映射关系不正确，请重新进行正确配置；如果映射关系正确故障仍然存在，请继续执行下面的步骤。

⑤ 在设备上执行 **display ip routing-table** 命令，查看公网上的所有路由，特别是所用的临时地址到 NAT 出接口需要配置好缺省路由。

第二篇

可靠性配置与管理



本篇介绍的是华为AR G3系列路由器中最常用的几种可靠性管理功能的配置与管理，具体包括以下几章内容。

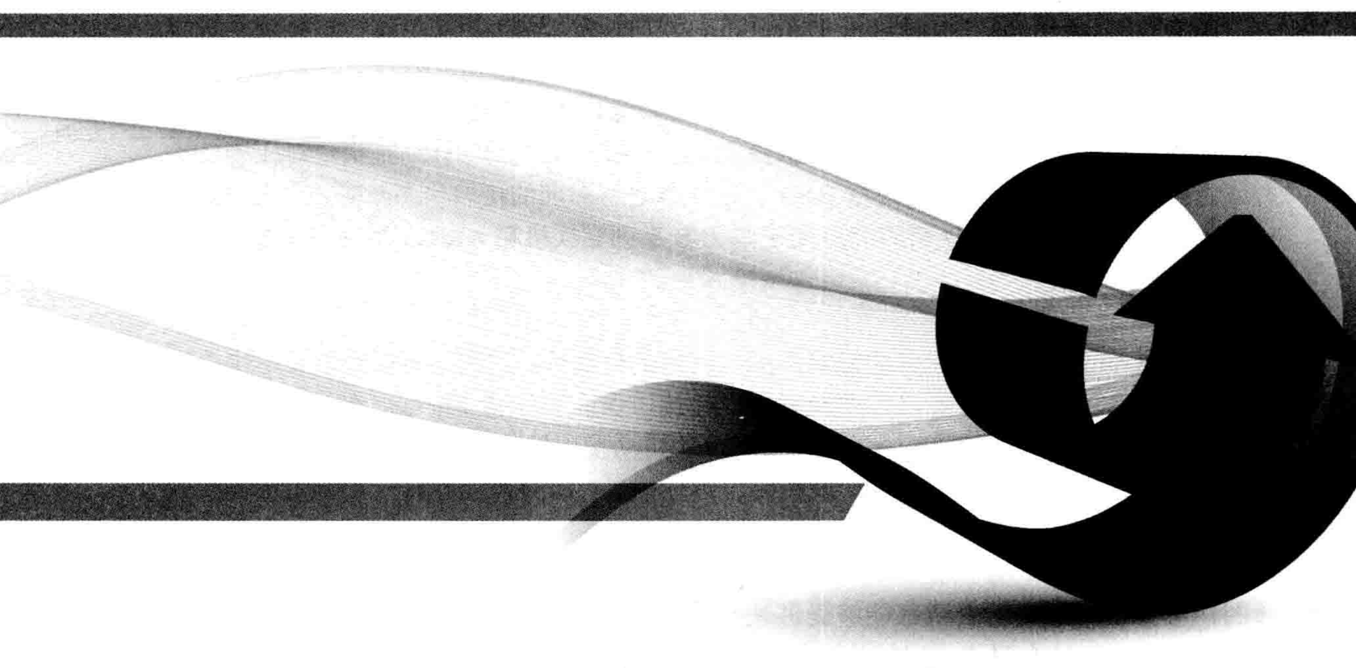
- 第7章　BFD和NQA配置与管理
- 第8章　VRRP配置与管理
- 第9章　接口备份和双机热备份配置与管理

第7章介绍的BFD（双向转发检测）和NQA（网络质量分析）是两种用于监督链路状态的检测机制，通过它们可以实现对设备上、下行链路故障的快速检测，以便及时发现链路故障并实现主、备链路切换。同时，BFD和NQA还可以与许多其他功能进行联动，如与接口状态、静态路由、RIP路由、OSPF路由、VRRP等，以弥补这些功能在动态检测能力上的不足。

第8章介绍的VRRP（虚拟主机冗余协议）是一种应用非常广泛的网关备份和负载均衡技术，通过它可以实现用户网络的多网关备份或负载均衡，主要应用于WAN接入线路的备份和负载均衡。它也可以与BFD和NQA进行联动配置。

第9章介绍的是另外两种备份技术，即路由器WAN接口和双主机热备份。其中接口备份是针对同一路由器上的多个WAN接口的备份，而双主机热备份则是针对位于同一网络位置的不同路由器的备份。相比VRRP技术仅应用于网关位置而言，这两种技术的应用更灵活、更广泛。接口备份功能可以与BFD和NQA进行联动配置，双机热备份功能可以与VRRP进行联动配置。

第7章 BFD和NQA配置与管理



在网络管理中，我们总是希望当网络中一些关键链路或者关键节点发生故障时能及时获得提示信息，并且希望系统最好能自动进行相应的应急处理，以便不影响正常的数据通信。本章介绍的BFD（双向转发检测）和NQA（网络质量分析）两种技术就能实现这样的非常实用的功能。

BFD不仅可以检测直连链路（也就是通常所说的“单跳”）的故障，还可以检测非直连链路（也就是通常所说的“多跳”）的故障。同时，它还可以与多种功能进行联动，如与接口状态、静态路由器、RIP路由、OSPF路由、IS-IS路由、BGP路由、VRRP等，在检测到故障后，上送到对应的上层应用模块进行快速处理。例如，与接口状态联动时就会把相应接口的状态由Up转Down；与各种路由联动时可以使这些路由管理模块进行重新拓扑计算，实现快速网络收敛；与VRRP联动时可以快速地切换到备用线路上。

NQA可以实时监视网络性能，在网络发生故障时进行故障诊断和定位。NQA支持DHCP测试、DNS测试、FTP测试、HTTP测试、ICMP测试、SNMP测试、TCP测试和Trace测试等，**本书仅介绍最常用的ICMP测试。**NQA通过发送测试报文，对网络性能或服务质量进行分析，为用户提供网络性能参数，如时延抖动、HTTP的总时延、通过DHCP获取IP地址的时延、TCP连接时延、FTP连接时延和文件传输速率等。NQA也可以与静态路由、VRRP、策略路由、接口等功能进行联动。

本章将详细介绍BFD自身的单跳和双跳检测机制，BFD检测参数、BFD与接口状态联动、单臂回声功能的配置与管理方法以及ICMP NQA测试示例的配置方法。至于BFD、NQA与其他功能的联动配置将在本书后面对应章节中再具体介绍。

7.1 BFD 基础

BFD（Bidirectional Forwarding Detection，双向转发检测）用于快速检测系统之间的发送和接收两个方向的通信故障，并在出现故障时通知上层应用。BFD 是一种提高网络可靠性的非常重要的技术，广泛应用于链路故障检测，并能实现与接口状态、静态路由、RIP 路由、IS-IS 路由、OSPF 路由和 BGP 路由、VRRP 等联动（联动是指使对应接口状态或者路由协议、VRRP 等可根据 BFD 会话状态进行对应的接口状态改变、路由收敛和 VRRP 主备切换等）。**BFD 可同时应用于华为 S 系列交换机和 AR G3 系列路由器。**

7.1.1 BFD 概述

为了减小设备故障对业务的影响，提高网络的可靠性，网络设备需要能够尽快检测到与相邻设备间的通信故障，以便及时采取措施，保证业务继续进行。在与网友的交流中也经常听到这样一些声音，说要是能让设备自动发现网络链路故障，并自动绕过故障链路重新进行拓扑收敛就好了。现在要告诉你的是，BFD 就是这样一种满足你需要的技术。

在现有网络中，有些链路通常是通过硬件检测信号（如 SDH 告警）来检测链路故障的，但并不是所有的介质都能够提供硬件检测功能。此外，还有依靠上层协议（如各种路由协议）自身的 Hello 报文机制来进行故障检测的，但是这些上层协议的 Hello 检测机制的检测时间通常都在 1 s 以上，这对某些关键应用来说是无法容忍的。同时，在一些小型三层网络中，如果没有部署路由协议，则无法使用路由协议的 Hello 报文机制来检测故障。

BFD 就是为了解决上述检测机制的不足而产生的，是一种通用的、标准化的与介质和协议均无关的快速链路故障检测机制，可为各上层协议（如路由协议、VRRP）等统一地快速检测两台路由器间（**不一定是直接连接的**）双向转发路径的故障。它是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况，保证邻居之间能够快速检测到通信故障，从而快速建立起备用通道恢复通信。

7.1.2 BFD 检测原理

如前所述，BFD 可在两台网络设备间建立用来监测设备间双向转发路径的 BFD 会话，为上层应用服务。但 BFD 本身并没有邻居发现机制，而是靠被服务的上层应用通知其邻居信息以建立会话。会话建立后会周期性地快速发送 BFD 报文，如果在检测时间内没有收到 BFD 报文则认为该双向转发路径发生了故障，通知被服务的上层应用进行相应的处理。下面以 OSPF 与 BFD 联动为例，简单介绍会话建立与故障检测工作流程。

1. *BFD 会话建立流程*

BFD 会话的建立有两种方式，即静态建立 BFD 会话和动态建立 BFD 会话。静态和动态创建 BFD 会话的主要区别在于本地标识符（Local Discriminator）和远端标识符（Remote Discriminator）的配置方式不同。标识符是用来标识对应 BFD 会话中本地和远端实体的数字标识，BFD 通过控制报文中的本地标识符和远端标识符区分不同的 BFD

会话。**当然，这个“本地”和“远端”是相对的，本地配置的远端标识符就是对端配置的本地标识符，本地配置的本地标识符也就是对端配置的远端标识符。**

（1）静态建立 BFD 会话

静态建立 BFD 会话是指通过命令行手动配置 BFD 会话参数，包括配置本地标识符和远端标识符等，然后手工下发 BFD 会话建立请求。

建立静态 BFD 会话又包括以下两种方式。

① 手动指定标识符的静态 BFD 会话

在这种 BFD 会话方式下，必须手动指定 BFD 会话的本地标识符和远端标识符。如果本端采用手动指定标识符，则对端也必须手动指定标识符。

② 标识符自协商的静态 BFD 会话

如果对端设备采用动态 BFD，而本端设备既要与之互通，又要能够实现 BFD 检测静态路由，则必须配置静态标识符自协商 BFD。**这种 BFD 会话方式无需指定本地标识符和远端标识符**。如果本端采用静态标识符自协商，则对端既可以配置静态标识符自协商，也可以配置动态 BFD。

（2）动态建立 BFD 会话

动态 BFD 联动主要是由各种路由协议（如 RIP、OSPF 等）触发的，具体将在本书后面介绍各种动态路由协议的章节进行介绍。在建立动态 BFD 会话时，系统对本地标识符和远端标识符分别采用如下处理方式。

① 动态分配本地标识符

当应用程序触发动态创建 BFD 会话时，系统分配本地动态会话标识符区域中可用的一个标识值作为本次 BFD 会话的本地标识符，然后向对端发送远端标识符的值为 0 的 BFD 控制报文（**之所以采用 0 来标识远端标识符，是因为在静态标识符配置中 0 是保留不能配置的**），进行会话协商。

② 自动学习远端标识符

当 BFD 会话的另一端收到远端标识符的值为 0 的 BFD 控制报文时，判断该报文是否与本地 BFD 会话匹配（查看 0 号标识符是否已被占用），如果匹配，则学习接收到的 BFD 本地标识符的值，以获取远端标识符，否则中断 BFD 会话。这种 BFD 会话方式主要用于与动态路由协议的联动中，并且同一时刻、同一链路只允许建立一组 BFD 会话。

图 7-1 所示为一个简单的 BFD 检测示例，RouterA 和 RouterB 两台设备上同时配置了 OSPF 与 BFD。总体来说，BFD 会话建立的基本流程如下所示（有关 OSPF 路由协议将在本书后面有详细介绍）。

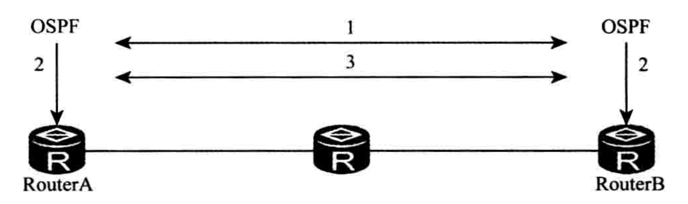


图 7-1　BFD 与 OSPF 联动会话建立流程示意图

① RouterA 和 RouterB 通过自己 OSPF 的 Hello 机制发现邻居并建立连接。

② OSPF 建立好新的邻居关系后，将相应的邻居信息（包括邻居的 IP 址和本设备的 IP 地址等）通告给本设备的 BFD 功能模块。

③ BFD 根据收到的邻居信息与对应邻居开始会话建立过程（BFD 会话的建立可以是以上介绍的静态建立和动态建立两种方式）。会话建立以后，BFD 才能开始检测链路状态，一旦出现故障可作出快速反应。

2. BFD 检测机制

BFD 的检测机制是先在两个系统间建立 BFD 会话，然后沿它们之间的路径周期性发送 BFD 控制报文，如果一方在既定的时间内没有收到对方发来的 BFD 控制报文或者自己发送的 BFD 报文返回（配置单臂回声功能时），则认为路径上发生了故障。

BFD 提供两种检测模式。

① 异步模式：BFD 的主要操作模式为异步模式。在这种模式下，系统之间相互周期性地单独发送 BFD 控制报文，如果某个系统在既定的时间内没有接收到对方发来的 BFD 报文，就认为此 BFD 会话的状态是 Down。

② 查询模式：当一个系统中存在大量 BFD 会话时，为防止周期性发送 BFD 控制报文的开销影响到系统的正常运行，可以采用查询模式。在查询模式下，一旦 BFD 会话建立，系统就不再周期性发送 BFD 控制报文，而是通过其他与 BFD 无关的机制检测连通性（比如路由协议的 Hello 机制、硬件检测机制等），从而减少 BFD 会话带来的开销。

现假设在图 7-1 所示的网络中，RouterB 检测到到达邻居 RouterA 的链路出现了故障，如图 7-2 所示，则 RouterA 和 RouterB 上的 BFD 功能会进行如下处理。

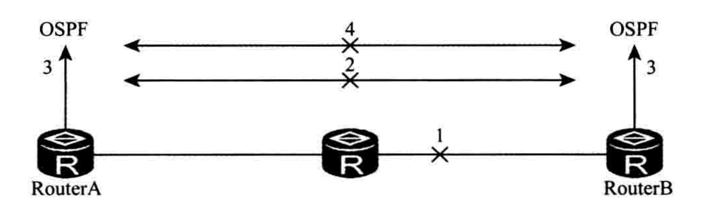


图 7-2 检测到故障时的 BFD 处理机制

① 通过 OSPF 的 Hello 机制，检测到链路出现故障（假设为 RouterB 与中间路由器之间的链路出现了故障）。

② RouterB 与 RouterA 之间的 BFD 会话状态首先变为 Down。

③ 然后，RouterB 与 RouterA 各自的 BFD 功能模块通知本地 OSPF 进程 BFD 邻居不可达。

④ 本地 OSPF 进程中断与对端设备的 OSPF 邻居关系，由 OSPF 协议进行重新拓扑计算，实现快速的网络收敛。

3. BFD 会话管理

BFD 会话有 4 种状态：Down、Init、Up 和 AdminDown。会话状态的变化通过 BFD 报文的 State 字段传递，系统根据自己本地的会话状态和接收到的对端 BFD 报文驱动状态改变。BFD 状态机的建立和拆除都采用三次握手机制，以确保两端系统都能知道状态的变化。下面仅以 BFD 会话建立为例，简单介绍状态机的迁移流程，如图 7-3 所示（仍以图 7-1 所示的网络为例）。

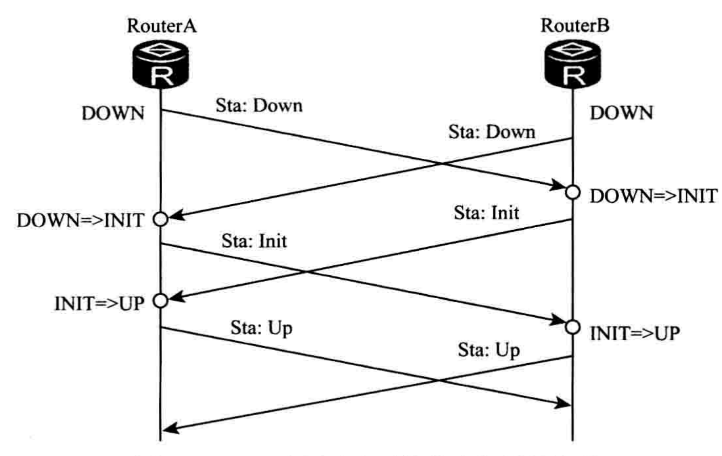


图 7-3　BFD 会话建立时的状态机迁移流程

① RouterA 和 RouterB 各自启动 BFD 状态机，初始状态为 Down，发送状态为 Down 的 BFD 报文。对于静态配置 BFD 会话，报文中的远端标识符的值是用户指定的；对于动态创建 BFD 会话，远端标识符的值是 0。

② RouterB 收到来自 RouterA 的状态为 Down 的 BFD 报文后，状态切换至 Init，并发送状态为 Init 的 BFD 报文，同时不再处理接收的状态为 Down 的 BFD 报文。同理，RouterA 在收到来自 RouterB 的状态为 Down 的 BFD 报文后，状态也切换至 Init，并发送状态为 Init 的 BFD 报文，也不再处理接收的状态为 Down 的 BFD 报文。

③ RouterB 在收到来自 RouterA 的状态为 Init 的 BFD 报文后，本地状态切换至 Up；RouterA 在收到来自 RouterB 的状态为 Init 的 BFD 报文后，本地状态切换至 Up。

当发现故障时，源端首先会向对端发送 AdminDown 状态的 BFD 报文，对端在收到这个报文会发送状态为 Down 的 BFD 报文（表明自己已关闭 BFD 会话），同时关闭本端的 BFD 会话。源端在收到对端发来的状态为 Down 的 BFD 报文后，源端 BFD 状态也变为 Down 状态，也会关闭自己的 BFD 会话。

7.2　BFD 主要应用

AR G3 系列路由器支持的 BFD 特性主要包括：单跳和多跳检测、静态标识符自协商 BFD、单臂回声功能、各种联动功能和 BFD 参数调整。下面分别予以简单介绍，至于 BFD 与各种路由协议的联动功能配置将在本书后面对应章节中具体介绍。

7.2.1　BFD 检测 IP 链路

在 IP 链路上建立 BFD 会话，可以利用 BFD 检测机制快速检测故障。BFD 检测 IP 链路支持单跳检测和多跳检测。

① BFD 单跳检测是指对两个直连系统进行 IP 连通性检测，“单跳”是 IP 链路的一跳。

② BFD 多跳检测是指 BFD 可以检测两个系统间的任意路径，这些路径可能跨越很多跳，也可能在某些部分发生重叠。

图 7-4 所示为 BFD 检测两台设备之间的 IP 单跳路径。此时，BFD 会话绑定本端的出接口，因为在直连情况下确定出接口后，相应要检测的到达对端设备的链路也就被唯一确定。

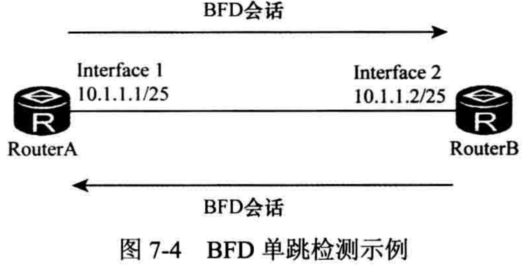


图 7-4 BFD 单跳检测示例

图 7-5 所示为 BFD 检测 RouterA 和 RouterC 之间的 IP 多跳路径。此时，BFD 会话绑定对端的 IP 地址，但不绑定本端出接口。因为在这种非直连情况下，绑定出接口不能唯一确定要检测的对端设备（因为中间可能还有多个设备），只有绑定了要监测设备的 IP 地址，才能最终唯一确定要检测所到达的设备。

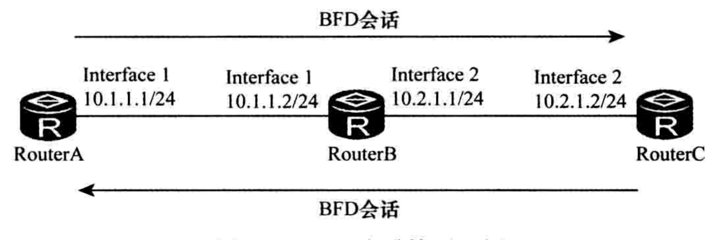


图 7-5 BFD 多跳检测示例

7.2.2 BFD 单臂回声功能

单臂回声功能是指通过 BFD 报文的环回操作来检测转发链路的连通性，主要应用于在两台直接连接的设备中只有一台支持 BFD 功能，另一台设备不支持 BFD 功能，但支持基本的网络层转发的情形下。也就是说，这种**单臂回声功能只适用于 BFD 单跳检测，且不支持二层设备间的链路检测**，即使是直接连接的。

为了能够快速地检测这样两台设备之间的故障，可在支持 BFD 功能的设备上配置单臂回声功能的 BFD 会话，主动发起回声请求功能，不支持 BFD 功能的设备接收到这样的 BFD 报文后会直接将其环回（**只作环回转发，不作其他任何处理**），从而实现转发链路的连通性检测功能。

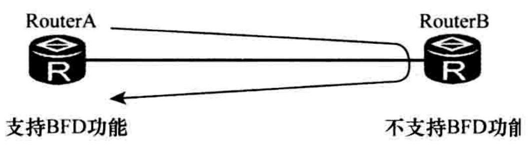


图 7-6 BFD 单臂回声功能应用示例

如图 7-6 所示，RouterA 支持 BFD 功能，RouterB 不支持 BFD 功能。在 RouterA 上配置单臂回声功能的 BFD 会话后，可以检测 RouterA 到 RouterB 之间的单跳路径。RouterB 接收到 RouterA 发送的 BFD 报文后，直接在网络层将该报文环回。通过这一特性，就可以实现快速检测 RouterA 和 RouterB 之间的直连链路的连通性。

7.2.3 BFD 与各种路由的联动

BFD 可以与静态路由、RIP 路由、OSPF 路由、IS-SI 路由、BGP 路由等进行联动。这里所说的“联动”就是指当发现某条路由所通过的路径上某条链路发生故障时，快速地通知路由管理功能模块及时进行相应的处理，重新进行路由计算，以实现快速拓扑收敛。

下面予以简单介绍。有关这些路由协议与 BFD 的联动配置将在本节后面对应章节介绍。

【经验之谈】其实除了静态路由外，其他各种动态路由本身都有邻居故障检测机制，如利用它们的 Hello 报文进行检测，但是 BFD 的检测效率更高，可实现更加快速的拓扑收敛。所以 BFD 与各种路由功能实现联动，是对这些路由（除静态路由外）的邻居检测机制的一种加强，并不是取代它们自身的各种 Hello 报文检测机制。

1. BFD 与静态路由联动

与各种动态路由协议不同，静态路由自身没有检测机制，当网络发生故障的时候，需要管理员介入。BFD 与静态路由联动特性可为公网静态路由绑定 BFD 会话，利用 BFD 会话来检测静态路由所在链路的状态。

BFD 与静态路由联动可为每条静态路由绑定一个 BFD 会话（当然，在实际情况中，是不会为每条静态路由配置 BFD 功能的，仅在一些关键静态路由中配置），当这条静态路由上绑定的 BFD 会话检测到链路故障（由 Up 转为 Down）后，BFD 会将故障上报路由管理系统，由路由管理模块将这条路由设置为“非激活”状态（表明此条路由不可用，并从 IP 路由表中删除该路由，**但在转发表 FIB 中仍然存在**）。当这条静态路由上绑定的 BFD 会话成功建立或者从故障状态恢复后（由 Down 转为 Up），BFD 又会上报路由管理模块，由路由管理模块将这条路由设置为“激活”状态（表明此路由可用，从 FIB 中重新加入 IP 路由表中）。

2. BFD 与 OSPF 联动

BFD 与 OSPF 联动就是将 BFD 和 OSPF 协议关联起来，通过 BFD 对链路故障的快速感应进而通知 OSPF 协议，从而加快 OSPF 协议对于网络拓扑变化的响应。OSPF 依靠自身的 Hello keepalive 定时器超时来检测链路故障的话，通常是在秒级，而利用 BFD 来检测的话，是在毫秒级。

如图 7-7 所示，RouterA 分别与 RouterC 和 RouterD 建立 OSPF 邻居关系，RouterA 到 RouterB 的路由出接口为 Interface 1，经过 RouterC 到达 RouterB。邻居状态到达 FULL 状态时通知 BFD 建立 BFD 会话。当 RouterA 和 RouterC 之间链路出现故障时，BFD 首先感知到并通知 RouterA。RouterA 处理邻居 Down 事件，重新进行路由计算，新的路由出接口为 Interface 2，经过 RouterD 到达 RouterB。

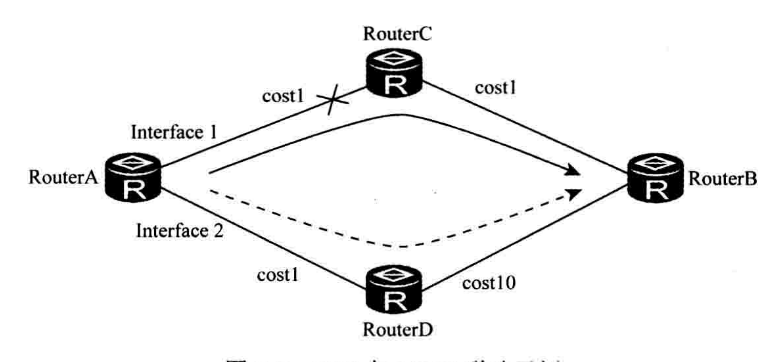


图 7-7　BFD 与 OSPF 联动示例

3. BFD 与 IS-IS 联动

通常情况下，IS-IS 设定发送 Hello 报文的时间间隔为 10 s，相邻设备失效的时间一般配置为 Hello 报文间隔的 3 倍。若在相邻设备失效时间内没有收到邻居发来的 Hello

报文，将会删除邻居。设备能感知到邻居故障的时间最小也是秒级。在高速的网络环境中，这将导致报文大量丢失。

BFD 与 IS-IS 联动是指 BFD 会话由 IS-IS 协议动态创建，不再依靠手动配置。当 BFD 检测到有故障时，通过路由管理模块通知 IS-IS 协议，由协议进行相应邻居 Down 处理，快速更新 LSP 信息和重新进行路由计算，从而实现 IS-IS 路由的快速收敛。但要注意的是，使用 BFD 并不是代替 IS-IS 协议本身的 Hello 机制，而是配合 IS-IS 协议更快地发现邻居方面出现的故障，并及时通知 IS-IS 重新计算相关路由以便正确指导报文的转发。

如图 7-8 所示，在各设备上使能了 IS-IS 功能，在 RouterA 和 RouterB 上配置了 BFD 与 IS-IS 联动。当 RouterA 和 RouterB 之间的链路故障时，BFD 能够快速检测到故障并通告给 IS-IS 协议。IS-IS Down 掉此接口的邻居，从而触发拓扑重新计算，同时更新 LSP 使得 RouterA 通过其他邻居（如 RouterC）能及时收到 RouterB 的更新 LSP，实现了网络拓扑的快速收敛。

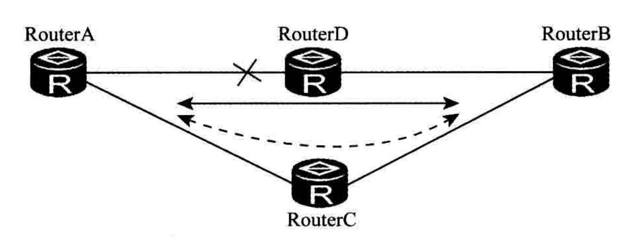


图 7-8 BFD 与 IS-IS 联动示例

4. BFD 与 BGP 联动

BGP 协议通过周期性地向对等体发送 Keepalive 报文来实现邻居检测机制，但这种机制检测到故障所需时间比较长，超过 1 s。当数据达到吉比特速率级别时，会导致大量的数据丢失。因此，BGP 协议通过引入 BFD 与 BGP 联动功能，利用 BFD 的快速检测机制，迅速发现 BGP 对等体间链路的故障，并报告给 BGP 协议，从而实现 BGP 路由的快速收敛。

如图 7-9 所示，RouterA 和 RouterB 分别属于 AS100 和 AS200，两台路由器直接相连并建立 EBGP 连接。使用 BFD 检测 RouterA 和 RouterB 之间的 BGP 邻居关系，当 RouterA 和 RouterB 之间的链路发生故障时，BFD 能够快速检测到故障并通告给 BGP 协议。

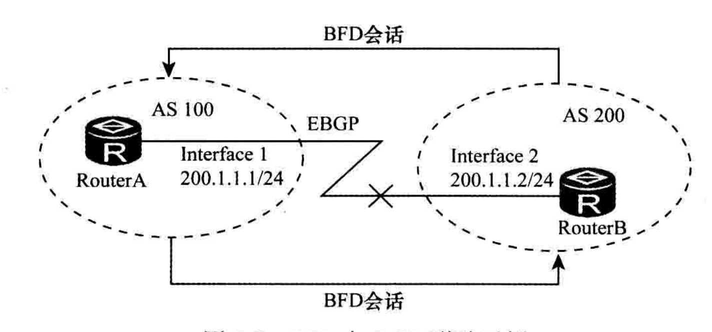


图 7-9 BFD 与 BGP 联动示例

7.2.4 BFD 的其他联动

BFD 除了可以与以上各种路由功能进行联动外，还可以与接口状态、VRRP、组播

PIM 联动等联动。下面分别予以简单介绍。

1. BFD 与接口状态联动

BFD 与接口状态联动提供一种简单的机制，使得 BFD 检测行为可以关联接口状态，提高了接口感应链路故障的灵敏度。在 BFD 与接口状态联动中，BFD 检测到链路故障后会立即上报 Down 消息到相应接口，使得接口进入一种特殊的 Down 状态，即 BFD Down 状态。该状态等效于链路协议 Down 状态，在该状态下只可以处理 BFD 报文，从而使该接口也可以快速感知链路故障，向系统日志发出告警信息。

如图 7-10 所示，链路中间存在其他设备，虽然三层仍是直连，但由于实际物理线路分段，一旦链路故障，两端设备需要比较长的时间才能检测到，导致直连路由收敛慢。如果在 RouterA 和 RouterB 上配置 BFD 会话的同时配置接口联动功能后，当 BFD 检测到链路出现故障时就会立即上报 Down 消息到相应接口，使接口进入 BFD Down 状态，该接口也可以快速感知链路故障，在控制台中向管理员提示告警信息。

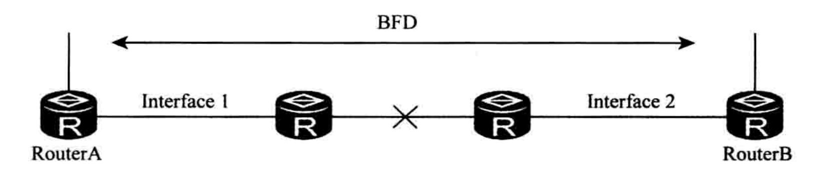


图 7-10　BFD 与接口状态联动示例

2. BFD 与 VRRP 联动

VRRP（虚拟路由冗余协议）的关键点是当 Master（主）设备出现故障时，Backup（备用）设备能够快速接替 Master 的转发工作，尽量缩短数据流的中断时间（**有关 VRRP 的基础工作原理和配置将在本书第 8 章介绍**）。

在没有采用 BFD 与 VRRP 联动机制前，当 Master 出现故障时，VRRP 依靠 Backup 设置的超时时间来判断是否应该抢占，切换速度在 1 s 以上。将 BFD 应用于 Backup 对 Master 的检测后，可以实现对 Master 故障的快速检测，缩短用户流量中断时间。BFD 对 Backup 和 Master 之间的实际地址通信情况进行检测，如果通信不正常，Backup 就认为 Master 已经不可用，可在 50 ms 以内自动升级成 Master，实现快速的主、备切换。

如图 7-11 所示，RouterA 和 RouterB 之间配置 VRRP 备份组建立主备关系，RouterA 为主用设备，RouterB 为备用设备，用户过来的流量从 RouterA 出去。当在 RouterA 和 RouterB 之间建立 BFD 会话后，VRRP 备份组监视该 BFD 会话，当 BFD 会话状态变为 Down 时，系统会自动通过修改备份组优先级实现主备快速切换。

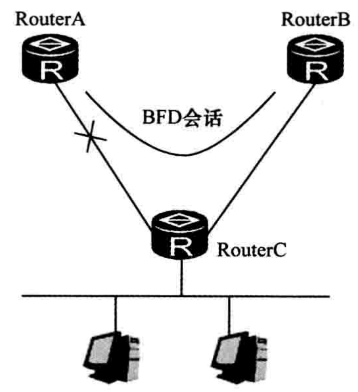


图 7-11　BFD 与 VRRP 联动示例

例如，当 BFD 检测到 RouterA 和 RouterC 之间的链路故障时，上报给 VRRP 一个 BFD 检测 Down 事件，RouterB 上 VRRP 备份组的优先级增加，增加后的优先级大于 RouterA 上的 VRRP 备份组的优先级，于是 RouterB 立刻升为 Master，后继的用户流量就会通过 RouterB 转发，从而实现 VRRP 的主备快速切换。

3. BFD 与 PIM 联动

在 PIM（协议相关模式）组播中，在没有采用 BFD 与 PIM 联动机制前，如果共享网段上的当前 DR（Designate Router，指定路由器）出现故障，其他 PIM 邻居会等到邻居关系超时才触发新一轮的 DR 竞选过程，组播数据传输中断的时间将比较长（通常是秒级）。有关 PIM 组播方面的基础知识和配置方面，请参见配套图书**《华为交换机学习指南》**。

BFD 与 PIM 联动的特点是可以进行快速故障检测，能够在毫秒级内通知 PIM 模块触发新一轮的 DR 竞选，而不是等到邻居关系超时。BFD 与 PIM 联动同时也适用于共享网段上 Assert（断言）竞选的过程，可以快速响应 Assert Winner 接口故障。

如图 7-12 所示，在与用户主机相连的共享网段上，RouterC 的下游接口 Interface1 和 RouterD 的下游接口 Interface2 之间建立 PIM BFD 会话，通过在链路两端发送 BFD 检测报文检测链路状态。RouterC 作为当前 DR，下游接口 Interface1 负责接收端组播数据的转发。若接口 Interface1 发生故障，BFD 快速把会话状态通告给组播路由模块，再由组播路由模块通告给 PIM。PIM 模块触发新一轮的 DR 竞选，最终 RouterD 作为新当选的 DR，这样下游接口 Interface2 可以在短时间内向接收端转发组播数据，从而缩小组播数据传输的中断时间。

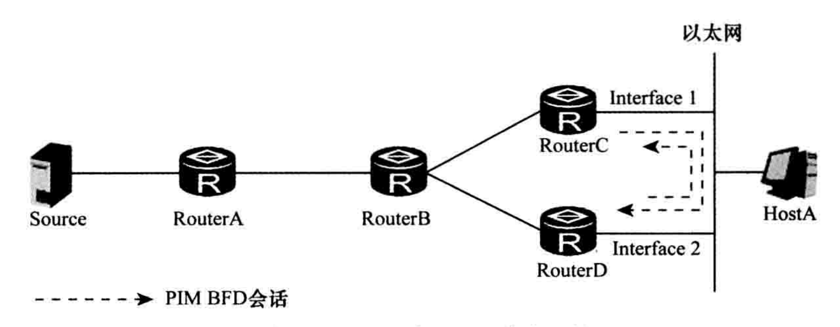


图 7-12　BFD 与 PIM 联动示例

7.3　BFD 配置与管理

本节介绍 AR G3 系列路由器中支持的一些基本 BFD 功能（包括单跳和多跳静态检测、静态标识符自协商 BFD、静态单臂回声功能、接口/子接口联动功能）和 BFD 参数调整的配置方法，至于与各种路由的联动功能相关的配置与管理方法，将在本书后面对应章节中介绍。

7.3.1　配置静态 BFD 单跳检测

单跳检测指检测**两台直连设备间**转发链路的 IP 连通性（也就是三层连通性，但接口可以是二层的），通过配置静态 BFD 单跳检测，**可实现直连链路的快速检测**。有关 BFD 单跳检测示例参见 7.2.1 小节的图 7-4。

在配置静态 BFD 单跳检测之前，需要配置接口的链路层协议参数，使接口的链路协议状态为 Up。另外，如果是三层接口，则还需要为接口配置 IP 地址。对于二层接口和三层接口的单跳检测配置方法有些区别，具体将在下面的配置中体现。

静态 BFD 单跳检测的主要配置任务如下。

① 使能设备上的全局 BFD 功能。

②（可选）配置 BFD 缺省组播 IP 地址。

③ 创建 BFD 会话的绑定信息，建立 BFD 组播会话。

④ 配置 BFD 会话的本端和远端标识符。

以上配置任务的具体配置步骤如表 7-1 所示（**注意：需要在直连设备两端同时配置**）。

表 7-1　静态 BFD 单跳检测的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图 缺省情况下，全局 BFD 功能处于未使能状态，可用 **undo bfd** 命令全局去使能 BFD 功能。执行 **undo bfd** 命令后，BFD 的所有功能将会关闭；如果已经配置了 BFD 会话信息，则所有的 BFD 会话的都会被删除
3	**default-ip-address** [*ip-address*] 例如：[Huawei-bfd] **default-ip-address** 224.0.0.150	（可选）配置 BFD 缺省组播 IP 地址，取值范围为 224.0.0.107～224.0.0.250。**仅当对端设备无法配置 IP 地址（如对端为二层设备）时采用** 【注意】如果 BFD 检测路径上存在重叠的 BFD 会话，例如，三层接口通过具有 BFD 功能的二层交换设备连接，不同 BFD 会话所在的设备必须配置不同的缺省组播 IP 地址，以避免 BFD 报文被错误地转发 缺省情况下，BFD 使用组播 IP 地址 224.0.0.184，可用 **undo default-ip-address** 命令恢复组播地址为缺省值。如果当前网络中存在其他协议使用该缺省组播地址，必须更改，**但如果已经配置了采用缺省组播地址的 BFD 会话，则不能再更改缺省组播地址**
4	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
5	**bfd** *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] 例如：[Huawei] **bfd** test **bind peer-ip** 1.1.1.2 **interface** gigabitethernet **1/0/0.1**	（二选一）对于三层接口，创建检测 IP 连通性的 BFD 会话绑定信息，并进入 BFD 会话视图。命令中的参数说明如下 • *session-name*：指定 BFD 会话的名称，1～15 个字符，不支持空格 • **peer-ip** *ip-address*：指定 BFD 会话绑定的对端 IP 地址 • **vpn-instance** *vpn-name*：可选参数，指定 BFD 会话绑定的 VPN 实例名称（该 VPN 实例必须已创建），1～31 个字符。如果不指定 VPN 实例，则认为对端 IP 地址是公共网络中的 IP 地址 • **interface** *interface-type interface-number*：指定绑定 BFD 会话的本端接口类型和接口编号。**单跳检测必须绑定对端 IP 地址和本端相应接口，下节将要介绍的多跳检测只需绑定对端 IP 地址**

（续表）

步骤	命令	说明
5	**bfd** *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] 例如：[Huawei] **bfd** test **bind peer-ip** 1.1.1.2 **interface** gigabitethernet **1/0/0.1**	• **source-ip** *ip-address*：可选参数，指定 BFD 报文携带的源 IP 地址。在 BFD 会话协商阶段，如果不配置该参数，则系统将在本地路由表中查找去往对端 IP 地址的出接口，然后以该出接口的 IP 地址作为本端发送 BFD 报文的源 IP 地址；在 BFD 会话检测链路阶段，如果不配置该参数，则系统会将 BFD 报文的源 IP 地址设置为一个固定的值。**通常情况下不需要配置该参数**，但当 BFD 与 URPF（Unicast Reverse Path Forwarding，单播逆向路径转发）特性一起应用时，由于 URPF 会对接收到的报文进行源 IP 地址检查，则用户需要手工配置 BFD 报文的源 IP 地址 【说明】在第一次创建单跳 BFD 会话时，必须绑定对端 IP 地址和本端相应接口，且创建后不可修改。如果需要修改，则只能删除后重新创建。在创建 BFD 配置项时，系统只检查 IP 地址是否符合 IP 地址格式，不检查其正确性，但绑定错误的对端 IP 地址或源 IP 地址都将导致 BFD 会话无法建立 目前，BFD 会话不会感知路由切换，所以如果绑定的对端 IP 地址改变引起路由切换到其他链路上，除非原链路转发不通，否则 BFD 不会重新协商 缺省情况下，未创建 BFD 会话绑定，可用 **undo bfd** *session-name* 命令删除指定的 BFD 会话，同时取消对应 BFD 会话的绑定信息
	bfd *session-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *ip-address*] 例如：[Huawei] **bfd** test **bind peer-ip default-ip interface** gigabitethernet 1/0/0.1	（二选一）对于二、三层接口和三层子接口，创建检测链路物理状态的 BFD 会话绑定，并进入 BFD 会话视图。命令中的 **peer-ip default-ip** 用来指定 BFD 会话绑定由本表第 3 步配置的缺省组播 IP，缺省情况下，组播缺省地址为 224.0.0.184。其他参数说明参见前面介绍的 **bfd** *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*]命令对应的参数 缺省情况下，未创建 BFD 会话绑定，可用 **undo bfd** *session-name* 命令删除指定的 BFD 会话，同时取消对应 BFD 会话的绑定信息 【注意】在三层接口或者三层子接口上创建组播 BFD 会话时，需要在三层接口上配置 IP 地址使其协议层 Up，否则，组播 BFD 会话无法协商成功
6	**discriminator local** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator local** 80	配置 BFD 会话的本地标识符，标识符用来区分两个系统之间的多个 BFD 会话，取值范围为 1～8 191 的整数 【注意】配置标识符时，本端的本地标识符与对端的远端标识符必需相同，否则 BFD 会话无法正确建立，**并且本地标识符和远端标识符配置成功后不可修改。对于使用缺省组播 IP 地址的 BFD 会话，本地标识符和远端标识符不能相同（其他情况下可以相同）** 静态 BFD 会话的本地标识符和远端标识符配置成功后，不可以修改。如果需要修改静态 BFD 会话本地标识符或者远端标识符，则必须先删除该 BFD 会话，然后配置本地标识符或者远端标识符

（续表）

步骤	命令	说明
7	**discriminator remote** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator remote** 80	配置 BFD 会话的远端标识符，标识符用来区分两个系统之间的多个 BFD 会话，取值范围为 1～8 191 的整数 其他注意事项参见上一步的 **discriminator local** *discr-value* 命令
8	**commit** 例如：[Huawei-bfd-session-test] **commit**	提交 BFD 会话配置。**无论改变任何 BFD 配置，必须执行本命令后才能使配置生效** 【说明】BFD 会话建立需要满足一定的条件，包括绑定的接口状态是 Up、有去往 peer-ip 的可达路由，在使用本命令提交配置时，如果当前不满足会话建立条件，系统将保留该会话的配置表项，但会话表项不能建立

7.3.2 配置静态 BFD 多跳检测

配置 BFD 多跳检测，可实现快速检测并监控网络中的多跳路径。在配置 BFD 多跳检测之前，需要配置路由协议，以保证 BFD 会话两端的设备路由可达。有关 BFD 单跳检测示例参见 7.2.1 小节的图 7-5。

总体来讲，静态 BFD 多跳检测的配置任务和配置方法与上节介绍的静态 BFD 单跳检测的配置任务和配置方法非常类似，主要不同体现在两个方面：一是不需要配置 BFD 缺省组播 IP 地址，因为多跳检测必须通过三层接口来实现，不能连接二层设备，**这也就决定了对端设备接口必须是配置了 IP 地址的三层接口或子接口，不能是二层接口**；二是在创建 BFD 会话绑定信息时仅需要指定要绑定的对端 IP 地址，不需要指定本端出接口。BFD 多跳检测的配置步骤如表 7-2 所示。

表 7-2　BFD 多跳检测的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图。其他说明参见 7.3.1 小节表 7-1 中的第 2 步
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	**bfd** *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**source-ip** *ip-address*] 例如：[Huawei] **bfd** test **bind peer-ip** 1.1.1.2	创建检测 IP 连通性的 BFD 会话绑定信息，并进入 BFD 会话视图。**在创建多跳 BFD 会话时，必须绑定对端 IP 地址**，其他说明参见 7.3.1 小节表 7-1 中的第 5 步
5	**discriminator local** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator local** 80	配置 BFD 会话的本地标识符。其他说明参见 7.3.1 小节表 7-1 中的第 6 步
6	**discriminator remote** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator remote** 80	配置 BFD 会话的远端标识符。其他说明参见 7.3.1 小节表 7-1 中的第 7 步
7	**commit** 例如：[Huawei-bfd-session-test] **commit**	提交 BFD 会话配置。其他说明参见 7.3.1 小节表 7-1 中的第 8 步

7.3.3 配置静态标识符自协商 BFD

如果对端设备采用动态 BFD，而本端设备既要与之互通，又要能够实现 BFD 检测静态路由，则必须配置静态标识符自协商 BFD。该功能主要用于检测采用静态路由实现三层互通的网络中。

在配置静态标识符自协商 BFD 之前需要为三层接口正确配置 IP 地址（**相连的必须是三层接口**）。配置静态标识符自协商 BFD 的具体步骤如表 7-3 所示。

表 7-3 静态标识符自协商 BFD 的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图。其他说明参见 7.3.1 小节表 7-1 中的第 2 步
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	**bfd** *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] **source-ip** *ip-address* **auto** 例如：[Huawei]**bfd** test **bind peer-ip** 10.1.1.2 **interface** gigabitethernet 1/0/0 **source-ip** 10.1.1.1 **auto**	创建静态标识符自协商 BFD 会话，并进入 BFD 会话视图。关键字 **auto** 用来使能静态标识符自协商功能。其他参数说明参见 7.3.1 小节表 7-1 中的第 5 步。但在创建静态标识符自协商 BFD 会话时：**必须配置源 IP 地址，必须指定明确的对端 IP 地址，不能使用组播 IP 地址** 【说明】在创建静态标识符自协商 BFD 会话时 ● 如果同时指定了对端 IP 地址和本端接口，则表示检测单跳链路，即检测以该接口为出接口、以 peer-ip 为下一跳地址的一条固定路由 ● 指定仅对端 IP 地址时，表示检测多跳链路 ● 如果用同时指定了对端 IP 地址、VPN 实例和本端接口，表示检测 VPN 路由的单跳链路 ● 如果仅同时指定了对端 IP 地址和 VPN 实例，则表示检测 VPN 路由的多跳链路 ● **source-ip** 参数用于保证在使能了 URPF 特性的情况下，使 BFD 报文不会被错误地丢弃。但该参数的配置必须正确，因为系统只检查该参数是否是合法的源 IP（例如，不能是组播或广播地址），不进行正确性检查 缺省情况下，未创建静态标识符自协商 BFD，可用 **undo bfd** *session-name* 命令删除指定的 BFD 会话，并取消 BFD 会话的绑定信息
5	**commit** 例如：[Huawei-bfd-session-test] **commit**	提交 BFD 会话配置。其他说明参见 7.3.1 小节表 7-1 中的第 8 步

7.3.4 配置静态 BFD 单臂回声功能

通过配置静态单臂回声功能，可实现快速检测并监控网络中的直连链路，**但相连的必须是三层接口**。在配置单臂回声功能之前需要为三层接口正确配置 IP 地址。静态 BFD 单跳回声功能的配置任务如下（有关 BFD 单臂回声功能及示例参见 7.2.2 小节的图 7-6）。

① 全局使能 BFD 功能。

② 建立静态单臂回声功能的 BFD 会话。

③ 配置会话标识符。

以上三项配置任务的具体配置步骤如表 7-4 所示。

表 7-4　静态 BFD 单跳回声功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图。其他说明参见 7.3.1 小节表 7-1 中的第 2 步
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	**bfd** *session-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*]**one-arm-echo** 例如：[Huawei] **bfd** test **bind peer-ip** 1.1.1.1 **interface** gigabitethernet 1/0/0 **one-arm-echo**	创建静态标识符自协商 BFD 会话，并进入 BFD 会话视图。关键字 **one-arm-echo** 用来建立单臂回声功能的 BFD 会话。其他参数说明参见 7.3.1 小节表 7-1 中的第 5 步 【注意】单臂回声功能的 BFD 会话只能应用在单跳检测中。但如果在单臂回声功能的 BFD 会话配置成功后，再修改出接口的 IP 地址，则 BFD 报文中的源 IP 地址不会更新，最终会影响回环 BFD 报文无法正确返回 缺省情况下，未配置单臂回声功能的 BFD 会话，可用 **undo bfd** *session-name* 命令删除指定的 BFD 会话，并取消 BFD 会话的绑定信息
5	**commit** 例如：[Huawei-bfd-session-test] **commit**	提交 BFD 会话配置。其他说明参见 7.3.1 小节表 7-1 中的第 8 步

7.3.5 配置静态 BFD 与接口/子接口状态联动

当直连链路中存在传输设备时，与接口本身的链路协议故障检测机制相比，BFD 能够更快地检测到链路故障。另外，对于 Eth-Trunk 或 VLANIF 等逻辑接口来说，链路协议状态是由其成员接口的链路协议状态决定的。因此，为了将 BFD 检测结果更快地通告给应用程序，在设备接口管理模块中为每个接口增加了一个属性，即 BFD 状态，即与该接口绑定的 BFD 会话的状态。系统根据接口的链路状态、协议状态和 BFD 状态决定接口的最终状态，并将结果通告给应用程序。

静态 BFD 会话状态与接口状态联动功能是指当 BFD 会话的状态变化时，直接修改接口或子接口（**可以是二层的，也可以是三层的**）的 BFD 状态。与接口或子接口状态联动的功能**仅针对绑定了出接口，且使用缺省组播 IP 地址进行检测的单跳检测 BFD 会话**，主要包括以下两方面。

1. BFD 会话状态与其绑定的接口状态联动

当 BFD 会话状态变为 Down 时，与其绑定的接口的 BFD 状态变为 Down，然后将接口状态通告给接口上的应用；当 BFD 会话的状态变为 Up 时，与其绑定的接口的 BFD 会话状态变为 Up。

2. BFD 会话状态与绑定接口的子接口状态联动

这种情况下，BFD 会话绑定的接口也必须是主接口。当主接口的 BFD 会话状态变

为 Down 时，与其绑定的主接口及其所有子接口的 BFD 状态都变为 Down，然后通告给各子接口上的应用程序；当主接口的 BFD 会话状态恢复为 Up 时，与其绑定的主接口及其所有子接口的 BFD 会话状态恢复为 Up。

静态 BFD 状态与接口/子接口状态联动的主要配置任务如下。

① 使能全局 BFD 功能。

②（可选）配置 BFD 缺省组播 IP 地址。

③ 创建静态 BFD 会话。

④ 配置静态 BFD 会话标识符。

⑤ 配置 BFD 会话与接口/子接口状态联动。

对比 7.3.1 小节介绍的静态单跳检测配置可以看出，BFD 会话状态与接口/子接口状态联动功能的配置与单跳 BFD 会话的配置差不多，只是在最后多了一个 BFD 会话与接口/子接口状态联动的配置。具体配置步骤如表 7-5 所示。

表 7-5　静态 BFD 会话状态与接口/子接口状态联动功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图。其他说明参见 7.3.1 小节表 7-1 的第 2 步
3	**default-ip-address** *ip-address* 例如：[Huawei-bfd]**default-ip-address** 224.0.0.150	（可选）配置 BFD 缺省组播 IP 地址，取值范围为 224.0.0.107～224.0.0.250。缺省情况下，BFD 使用组播地址 224.0.0.184。其他说明参见 7.3.1 小节表 7-1 的第 3 步
4	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
5	**bfd** *session-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *ip-address*] 例如：[Huawei] **bfd** test **bind peer-ip default-ip interface** gigabitethernet 1/0/0.1	创建检测链路物理状态的 BFD 会话绑定，并进入 BFD 会话视图。关键字 **peer-ip default-ip** 用来指定 BFD 会话绑定缺省组播 IP 地址，**必须使用缺省组播 IP 地址进行绑定，且必须同时指定出接口（且必须是主接口）**。其他说明参见 7.3.1 小节表 7-1 的第 5 步
6	**discriminator local** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator local** 80	配置 BFD 会话的本地标识符，标识符用来区分两个系统之间的多个 BFD 会话，取值范围为 1～8 191 的整数。其他说明参见 7.3.1 小节表 7-1 的第 6 步
7	**discriminator remote** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator remote** 80	配置 BFD 会话的远端标识符，标识符用来区分两个系统之间的多个 BFD 会话，取值范围为 1～8 191 的整数。其他说明参见 7.3.1 小节表 7-1 的第 7 步
8	**process-interface-status**（与接口联动） 或 **process-interface-status sub-if**（与子接口联动） 例如：[Huawei-bfd-session-test] **process-interface-status**	配置当前 BFD 会话与其绑定接口或子接口状态联动 【注意】只能对采用缺省组播 IP 地址检测的单跳 BFD 会话配置本命令，支持 BFD 会话绑定主接口或子接口。如果有多个 BFD 会话绑定到同一个接口，只能在一个会话中使能 **process-interface-status**，即**只能有一个会话的状态会改变绑定接口或子接口的 BFD 状态** 缺省情况下，BFD 会话不与绑定的接口或子接口进行状态联动，即 BFD 会话状态的变化不修改接口管理模块中的接口或子接口状态，可用 **undo process-interface-status** 命令恢复缺省设置

（续表）

步骤	命令	说明
9	**commit** 例如：[Huawei-bfd-session-test] **commit**	提交 BFD 会话配置。当 BFD 会话状态变为 Down 时，与会话绑定的主接口及其子接口的 BFD 状态都会变为 Down 其他说明参见 7.3.1 小节表 7-1 的第 8 步

7.3.6 调整 BFD 参数

通过调整 BFD 检测参数，可使 BFD 会话更快速地检测和监控网络中的链路。但在调整 BFD 参数之前，需要完成前面对应情形下的 BFD 会话创建。可调的 BFD 参数包括 BFD 检测时间、BFD 等待恢复时间、BFD 会话描述信息、BFD 会话延迟 Up 功能和全局 TTL 功能。调整 BFD 检测参数的具的配置步骤如表 7-6 所示（各参数配置没有严格的先后次序），**但因为各参数都有其对应的缺省值，故这些参数可根据实际需要选择配置。**

表 7-6　　调整 **BFD** 参数的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** *session-name* 例如：[Huawei] **bfd** test	进入指定的 BFD 会话视图
3	**min-tx-interval** *interval* 例如：[Huawei-bfd-session-test] **min-tx-interval** 1000	配置 BFD 报文的发送间隔，取值范围为 10～2 000 ms 【说明】用户可以根据网络的实际状况增大或者降低 BFD 报文的发送间隔。BFD 报文的发送间隔直接决定了 BFD 会话的检测时间。对于不太稳定的链路，如果配置的 BFD 报文的发送间隔较小，则 BFD 会话可能会发生振荡，这时可以选择增大 BFD 报文的发送间隔。**通常情况下，建议使用缺省值，不随意修改发送间隔。**如果 BFD 会话在设置的检测周期内没有收到对端发来的 BFD 报文，则认为链路发生了故障，BFD 会话的状态将会置为 Down。为降低对系统资源的占用，一旦检测到 BFD 会话状态变为 Down，系统自动将本端的发送间隔调整为大于 1 000 ms 的一个随机值，当 BFD 会话的状态重新变为 Up 后，再恢复成用户配置的时间间隔 缺省情况下，BFD 报文的发送间隔是 1 000 ms，可用 **undo min-tx-interval** 命令恢复 BFD 报文的发送间隔为缺省值
4	**min-rx-interval** *interval* 例如：[Huawei-bfd-session-test] **min-rx-interval** 500	配置 BFD 报文的接收间隔，取值范围为 10～2 000 ms，通常是要小于上一步配置的 BFD 报文发送时间间隔 缺省情况下，BFD 报文的接收间隔是 1 000 ms，可用 **undo min-rx-interval** 命令恢复 BFD 报文的接收间隔为缺省值
5	**detect-multiplier** *multiplier* 例如：[Huawei-bfd-session-test] **detect-multiplier** 10	配置本地检测倍数，取值范围为 3～50 的整数 【说明】BFD 会话的本端检测倍数直接决定了对端 BFD 会话的检测时间，检测时间=接收到的远端 Detect Multi × max（本地的 RMRI，接收到的 DMTI），其中，Detect Mult（Detect time multiplier）是检测倍数，通过本条命令配置；RMRI（Required Min Rx Interval）是本端能够支持的最短

（续表）

步骤	命令	说明
5	**detect-multiplier** *multiplier* 例如：[Huawei-bfd-session-test] **detect-multiplier** 10	BFD 报文接收间隔，通过本表第 3 步 **min-rx-interval** 命令配置的；DMTI（Desired Min Tx Interval）是本端想要采用的最短 BFD 报文的发送间隔，是通过本表第 4 步 **min-tx-interval** 命令配置的 缺省情况下，本地检测倍数为 3，可用 **undo detect-multiplier** 命令恢复 BFD 会话的本地检测倍数为缺省值
6	**wtr** *wtr-value* 例如：[Huawei-bfd-session-test] **wtr** 30	配置 BFD 会话的等待恢复时间，取值范围为 1～60 min 【注意】如果 BFD 会话发生振荡，则与之关联的应用将在主备之间频繁切换。为避免这种情况的发生，可以配置 BFD 会话的等待恢复时间 WTR。当 BFD 会话从状态 Down 变为状态 Up 时，BFD 等待 WTR 超时后才将这个变化通知给上层应用，但其他状态变化的事件仍立即上报，不受 WTR 影响。**需要在两端配置相同的 WTR**，否则，当一端会话状态变化时，两端应用程序感知到的 BFD 会话状态将不一致 缺省情况下，WTR 为 0，即不等待，可用 **undo wtr** 命令取消 BFD 会话的等待恢复时间为缺省值
7	**description** *description* 例如：[Huawei-bfd-session-test] **description** RouterA_to_RouterB	配置 BFD 会话的描述信息，方便用户识别具体的 BFD 会话。如果用户需要识别不同的 BFD 会话，可以配置 BFD 会话的描述信息对 BFD 会话监视的链路进行简单描述。参数 *description* 用来配置 BFD 会话的描述信息，1～51 个字符，支持空格，区分大小写 【注意】**本命令仅对静态配置的 BFD 会话有效**，对于动态配置的 BFD 会话和静态标识符自协商 BFD 会话无效。且如果已经配置了 BFD 会话的描述信息，则再次执行本命令后，原来的描述信息将被覆盖，此时不会有任何的提示信息 缺省情况下，BFD 会话的描述信息是空，可用 **undo description** 命令删除 BFD 会话的描述信息
8	**quit** 例如：[Huawei-bfd-session-test] **quit**	退出 BFD 会话视图，返回系统视图
9	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能并进入 BFD 视图 缺省情况下，全局 BFD 功能未使能，可用 **undo bfd** 命令全局去使能 BFD 功能。执行 **undo bfd** 命令后，BFD 的所有功能将会关闭。如果已经配置了 BFD 会话信息，则所有的 BFD 会话都会被删除
10	**delay-up** *time* 例如：[Huawei-bfd] **delay-up** 100	配置 BFD 会话延迟 Up 的时间，取值范围为 1～600 整数秒 【说明】在实际组网环境中，一些设备只根据 BFD 会话是否 Up 来启动流量切换。由于路由协议 Up 的时间比接口 Up 的时间晚，这样可能导致流量回切时查不到路由，从而导致流量丢失。为避免这种情况的发生，需要 BFD 会话在建立并协商 Up 之前通过本命令延迟一段时间。但本命令只影响系统中所有未提交 BFD 配置的会话。对于已经创建的 BFD 会话，会话状态变化时如果要再次协商 Up，则会延迟用户配置的时间间隔 缺省情况下，BFD 会话延迟 Up 的时间是 0 s，可用 **undo delay-up** 命令取消延迟 BFD 会话 Up 的功能

（续表）

步骤	命令	说明
11	**peer-ip** *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** } *ttl-value* 例如：[Huawei-bfd] **peer-ip** 1.1.1.0 24 **ttl single-hop** 254	配置 BFD 报文的生存时间。使用某些不同 VRP 系统版本的设备进行互通时，BFD 会话双方 TTL 设置及检测方法不一致时可能会导致报文被丢弃。为了使不同版本的设备能够互通，并考虑后续版本升级以及和其他厂商的设备互通，此时可通过本命令配置全局 TTL 功能。命令中的参数和选项说明如下。 • *peer-ip*：指定 BFD 会话绑定的对端 IP 地址 • *mask-length*：指定 BFD 会话绑定的对端 IP 地址的子网掩码长度，取值范围为 8～32 的整数 • **single-hop**：二选一选项，指定所配置的 BFD 报文生存时间的 BFD 会话为单跳会话类型 • **multi-hop**：二选一选项，指定所配置的 BFD 报文生存时间的 BFD 会话为多跳会话类型 • *ttl-value*：指定 BFD 报文的 TTL 值，取值范围为 1～255 的整数 【注意】在配置 BFD 报文的生存时间时要注意以下几个方面。 • IP 网段地址必须和指定的掩码长度相匹配，长掩码的配置会优先于短掩码的配置 • 对不同 BFD 会话中的 BFD 报文生存时间不能配置 IP 网段地址、掩码长度、TTL 值类型这三者都相同 • 对于同一 IP 地址、同一掩码，单跳类型的 TTL 值必须大于多跳类型的 TL 值 • 当配置的会话较多时，更新对应会话的 TTL 值会比较耗费时间，若多次配置之间的时间间隔太短，系统将会提示当前会话更新正在进行，请稍后配置 • 配置同一 IP 网段地址的多跳 TTL 值后，会对设备单跳动态会话造成影响，此时应该增加同一 IP 地址、长掩码（长于多跳 TTL 配置掩码）、单跳类型的 TTL 值配置 缺省情况下，不配置 BFD 报文的生存时间，采用缺省值。对于静态配置的 BFD 会话，单跳 BFD 报文的生存时间为 255，多跳 BFD 报文的生存时间为 254；对于动态建立的 BFD 会话，单跳 BFD 报文的生存时间为 255，多跳 BFD 报文的生存时间为 253

7.3.7 BFD 管理

配置好 BFD 功能后，可通过以下 **display** 任意视图命令检查配置结果，查看已配置的 BFD 会话的情况，也可用以下 **reset** 用户视图命令清除 BFD 会话统计信息。

① **display bfd interface** [*interface-type interface-number*]：查看使能了 BFD 功能的指定接口或者所有接口的信息。

② **display bfd session** { **all** | **static** | **discriminator** *discr-value* | **dynamic** | **peer-ip** { **default-ip** | *peer-ip* [**vpn-instance** *vpn-instance-name*] } | **static-auto** } [**verbose**]：查看符合指定条件或者所有 BFD 会话信息。

③ **display bfd statistics**：查看 BFD 全局统计信息。

④ **display bfd statistics session** { **all** | **static** | **dynamic** | **discriminator** *discr-value* | **peer-ip default-ip** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] | **static-auto** }：查看符合指定条件或者所有 BFD 会话统计信息。

⑤ **reset bfd statistics** { **all** | **discriminator** *discr-value* }：清除指定标识符或者所有 BFD 会话的统计信息。

7.4 BFD 配置示例

为了加深对上述各种 BFD 检测配置的理解，下面通过一些具体示例介绍它们的具体配置方法。

7.4.1 单跳检测二层链路配置示例

本示例的基本拓扑结构如图 7-13 所示，RouterA 和 RouterB 通过二层接口连通。用户希望可以实现设备间链路故障的快速检测。

本示例很简单，仅需在 RouterA 和 RouterB 上分别配置 BFD 会话，实现 RouterA 和 RouterB 间链路的检测。但要注意的是，因为本示例是通过**二层接口相连的单跳检测**，所以需要配置缺省的 BFD 组播 IP 地址，同时在创建 BFD 会话绑定时一定要指定出接口。具体配置步骤如下。

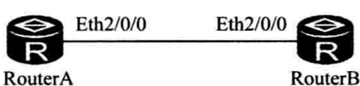


图 7-13 BFD 单跳检测二层链路示例拓扑结构

1. RouterA 上的配置

① 使能 RouterA 上的全局 BFD 功能。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] bfd
[RouterA-bfd] quit
```

② 配置 RouterA 上的 BFD 会话。注意要同时配置缺省 BFD 组播 IP 地址和指定出接口，此处所采用的是缺省 BFD 组播 IP 地址 224.0.0.184。

```
[RouterA] bfd atob bind peer-ip default-ip interface ethernet 2/0/0  !---创建一个名为 atob 的 BFD 会话绑定信息
[RouterA-bfd-session-atob] discriminator local 1  !---配置本地标识符为 1，与 RouterB 上配置的远端标识符一致
[RouterA-bfd-session-atob] discriminator remote 2  !---配置远端标识符为 2，与 RouterB 上配置的本地标识符一致
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

2. RouterB 上的配置

① 使能 RouterB 上的全局 BFD 功能。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] bfd
[RouterB-bfd] quit
```

② 配置 RouterB 上的 BFD 会话。一样要同时配置缺省 BFD 组播 IP 地址和指定出接口，同样此处所采用的是缺省 BFD 组播 IP 地址 224.0.0.184（没有做更改配置）。

```
[RouterB] bfd btoa bind peer-ip default-ip interface ethernet 2/0/0
[RouterB-bfd-session-btoa] discriminator local 2
```

```
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置好后在 RouterA 和 RouterB 上分别执行 **display bfd session all verbose** 命令可看到建立了一个单跳（**One Hop**）检测的 BFD 会话，且会话状态为 Up。下面是 RouterA 上的输出示例。

```
<RouterA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4097         (One Hop) State : Up          Name : atob
--------------------------------------------------------------------------------
  Local Discriminator     : 1                  Remote Discriminator    : 2
  Session Detect Mode     : Asynchronous Mode Without Echo Function
  BFD Bind Type           : Interface(Ethernet2/0/0)
  Bind Session Type       : Static
  Bind Peer IP Address    : 224.0.0.184
  NextHop Ip Address      : 224.0.0.184
  Bind Interface          : Ethernet2/0/0
  FSM Board Id            : 0                  TOS-EXP                 : 7
  Min Tx Interval (ms)    : 1000               Min Rx Interval (ms)    : 1000
  Actual Tx Interval (ms): 1000                Actual Rx Interval (ms): 1000
  Local Detect Multi      : 3                  Detect Interval (ms)    : 3000
  Echo Passive            : Disable            Acl Number              : -
  Destination Port        : 3784               TTL                     : 255
  Proc Interface Status   : Disable            Process PST             : Disable
  WTR Interval (ms)       : -
  Active Multi            : 3
  Last Local Diagnostic   : No Diagnostic
  Bind Application        : No Application Bind
  Session TX TmrID        : -                  Session Detect TmrID    : -
  Session Init TmrID      : -                  Session WTR TmrID       : -
  Session Echo Tx TmrID   : -
  PDT Index               : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description     : -
--------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 1/0
```

现对 RouterA 的 Eth2/0/0 接口执行 **shutdown** 命令操作，模拟链路故障。配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令即可看到建立了一个单跳检测的 BFD 会话，且会话状态为 Down。下面是 RouterA 上的输出示例。

```
<RouterA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4097         (One Hop) State : Down        Name : atob
--------------------------------------------------------------------------------
  Local Discriminator     : 1                  Remote Discriminator    : 2
  Session Detect Mode     : Asynchronous Mode Without Echo Function
  BFD Bind Type           : Interface(Ethernet2/0/0)
  Bind Session Type       : Static
  Bind Peer IP Address    : 224.0.0.184
  NextHop Ip Address      : 224.0.0.184
  Bind Interface          : Ethernet2/0/0
<略>
--------------------------------------------------------------------------------
```

```
Total UP/DOWN Session Number : 0/1
```

7.4.2 VLANIF 接口 BFD 单跳检测配置示例

如图 7-14 所示，RouterA 和 RouterB 通过 VLANIF 接口实现三层互通。用户希望可以实现设备间链路故障的快速检测。

VLANIF100 10.1.1.5/24 Eth2/0/0 RouterA —— VLANIF100 10.1.1.6/24 Eth2/0/0 RouterB

图 7-14 VLANIF 接口 BFD 单跳检测示例拓扑结构

本示例与上节介绍的示例差不多，唯一不同的是本示例中是检测三层 VLANIF 接口的状态，所以在创建 BFD 会话绑定信息时要绑定对端的 IP 地址（不使用 BFD 组播 IP 地址），同时因为也是单跳检测，所以也要指定出接口。当然首先要把直连的两个物理接口加入对应的 VLAN 中，然后为两端 VLANIF 接口配置 IP 地址（通常直连两端是采用同一网段 IP 地址的）。下面仅介绍两端的 BFD 相关配置。

1. RouterA 上的配置

① 使能 RouterA 上的全局 BFD 功能。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] bfd
[RouterA-bfd] quit
```

② 配置 RouterA 上的 BFD 单跳检测会话。要指定具体的对端 IP 地址和出接口。

```
[RouterA] bfd atob bind peer-ip 10.1.1.6 interface vlanif 100
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterB-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

2. RouterB 上的配置

① 使能 RouterB 上的全局 BFD 功能。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] bfd
[RouterB-bfd] quit
```

② 配置 RouterB 上的 BFD 会话，也要指定具体的对端 IP 地址和出接口。

```
[RouterB] bfd btoa bind peer-ip 10.1.1.5 interface vlanif 100
[RouterB-bfd-session-btoa] discriminator local 2
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置完成后，同样可在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，此时可以看到建立了一个单跳检测的 BFD 会话，且会话状态为 Up。具体输出示例略。

也可对 RouterA 的 Eth2/0/0 接口执行 **shutdown** 操作，模拟链路故障。配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳检测的 BFD 会话，且会话状态为 Down。具体输出示例略。

7.4.3 BFD 多跳检测配置示例

本示例的基本拓扑结构如图 7-15 所示，RouterA 和 RouterC 为非直连设备，通过配

置静态路由互通。用户希望可以实现对设备间链路故障的快速检测。

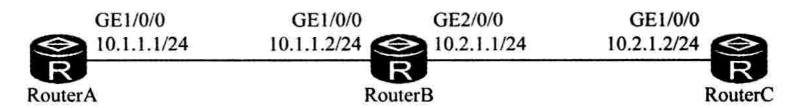


图 7-15　BFD 多跳检测配置示例的拓扑结构

因为本示例中 RouterA 和 RouterC 并不是直接连接的，所以需要配置 BFD 多跳检测，在 RouterA 和 RouterC 上分别配置 BFD 会话，以实现 RouterA 到 RouterC 间多跳路径的检测。根据 7.3.2 小节介绍的配置方法可以得出以下具体配置方法。

① 配置静态路由，使 RouterA、RouterC 之间有可达路由。需要同时在 RouterA 和 RouterC 上配置。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] ip route-static 10.2.0.0 16 10.1.1.2   !---这里采用 16 位掩码的汇总静态路由方式进行配置
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] ip route-static 10.1.0.0 16 10.2.1.1
```

② 在 RouterA 上配置与 RouterC 之间的多跳检测 BFD 会话。因为是多跳检测，所以配置时不要指定出接口，但要指定对端 IP 地址。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atoc bind peer-ip 10.2.1.2
[RouterA-bfd-session-atoc] discriminator local 10
[RouterA-bfd-session-atoc] discriminator remote 20
[RouterA-bfd-session-atoc] commit
[RouterA-bfd-session-atoc] quit
```

③ 在 RouterC 上配置与 RouterA 之间的多跳检测 BFD 会话。同样，配置时不要指定出接口，但要指定对端 IP 地址。

```
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] bfd ctoa bind peer-ip 10.1.1.1
[RouterC-bfd-session-ctoa] discriminator local 20
[RouterC-bfd-session-ctoa] discriminator remote 10
[RouterC-bfd-session-ctoa] commit
[RouterC-bfd-session-ctoa] quit
```

配置完成后，在 RouterA 和 RouterC 上执行 **display bfd session all verbose** 命令，可以看到建立了一个多跳（**Multi Hop**）BFD 会话，且状态为 Up。下面是 RouterA 上的输出示例。

```
<RouterA> display bfd session all verbose
--------------------------------------------------------------------------
Session MIndex : 256          (Multi Hop) State :Up          Name : atoc
--------------------------------------------------------------------------
  Local Discriminator      : 10                Remote Discriminator      : 20
  Session Detect Mode      : Asynchronous Mode Without Echo Function
  BFD Bind Type              : Peer Ip Address
  Bind Session Type        : Static
  Bind Peer Ip Address     : 10.2.1.2
  Track Interface          : -
```

```
FSM Board Id              : 0              TOS-EXP                  : 7
Min Tx Interval (ms)      : 1000           Min Rx Interval (ms)     : 1000
Actual Tx Interval (ms): 1000              Actual Rx Interval (ms): 1000
Local Detect Multi        : 3              Detect Interval (ms)     : 3000
Echo Passive              : Disable        Acl Number               : -
Destination Port          : 3784           TTL                      : 254
Proc interface status     : Disable        Process PST              : Disable
WTR Interval (ms)         : -
Active Multi              : 3
Last Local Diagnostic     : No Diagnostic
Bind Application          : No Application Bind
Session TX TmrID          : -              Session Detect TmrID     : -
Session Init TmrID        : -              Session WTR TmrID        : -
Session Echo Tx TmrID     : -
PDT Index                 : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description       : -
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

对 RouterA 的 GE1/0/0 接口执行 **shutdown** 操作，模拟链路故障。配置完成后，在 RouterA 和 RouterC 上执行 **display bfd session all verbose** 命令，可以看到建立了一个多跳检测的 BFD 会话，且会话状态为 Down。输出示例略。

7.4.4 BFD 状态与接口状态联动配置示例

如图 7-16 所示，RouterA 和 RouterB 网络层直连，链路中间存在二层传输设备 SwitchA 和 SwitchB。用户希望两端设备能够快速感知到链路故障，触发路由快速收敛。

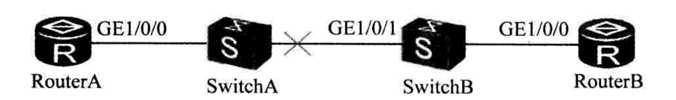


图 7-16 BFD 状态与接口状态联动配置示例的拓扑结构

在本示例中，两个路由器中间是两台二层交换机，所以两个路由器与交换机连接的接口也必须是二层的，必须把它们加入对应的 VLAN 中。然后在 RouterA 和 RouterB 上分别配置 BFD 会话，以实现 RouterA 和 RouterB 间链路的检测，当 BFD 会话状态 Up 以后分别在 RouterA 和 RouterB 上配置 BFD 状态与接口状态联动。下面是具体的配置步骤。

① 把 RouterA 和 RouterB 的 GE1/0/0 接口加入对应的 VLAN 中（这里仅以最简单的，同属于 VLAN10 的情形为例进行介绍）。

```
<Router> system-view
[Router] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] port link-type trunk
[RouterA-GigabitEthernet1/0/0] port trunk pvid vlan 10
[RouterA-GigabitEthernet1/0/0] quit
<Router> system-view
[Router] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] port link-type trunk
[RouterB-GigabitEthernet1/0/0] port trunk pvid vlan 10
[RouterB-GigabitEthernet1/0/0] quit
```

② 在 RouterA 上使能 BFD，配置与 RouterB 之间的 BFD 会话。注意：这里需要使用缺省的组播 BFD IP 地址，并要指定出接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterA-bfd-session-atob] discriminator local 10
[RouterA-bfd-session-atob] discriminator remote 20
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

③ 在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD 会话。同样需要使用缺省的组播 BFD IP 地址，并要指定出接口。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterB-bfd-session-btoa] discriminator local 20
[RouterB-bfd-session-btoa] discriminator remote 10
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳的 BFD Session，状态为 Up，但是“Proc interface status”字段显示为“Disable”，表明还没配置 **process-interface-status** 命令（如果已配置该命令，则显示为 Enable）。以下是 RouterA 上的输出示例。

```
[RouterA] display bfd session all verbose
--------------------------------------------------------------------------------
  Session MIndex : 16384        (One Hop) State : Up         Name : atob
--------------------------------------------------------------------------------
  Local Discriminator      : 10                   Remote Discriminator     : 20
  Session Detect Mode      : Asynchronous Mode Without Echo Function
  BFD Bind Type            : Interface(GigabitEthernet1/0/0)
  Bind Session Type        : Static
  Bind Interface           : GigabitEthernet1/0/0
  FSM Board Id             : 3                    TOS-EXP                  : 7
  Min Tx Interval (ms)     : 10                   Min Rx Interval (ms)     : 10
  Actual Tx Interval (ms): 10                     Actual Rx Interval (ms): 10
  Local Detect Multi       : 3                    Detect Interval (ms)     : 30
  Echo Passive             : Disable              Acl Number               : --
  Destination Port         : 3784                 TTL                      : 255
  Proc interface status    : Disable              Process PST              : Disable
  WTR Interval (ms)        : 300000
  Active Multi             : 3
  Last Local Diagnostic    : No Diagnostic
  Bind Application         : No Application Bind
  Session TX TmrID         : --                   Session Detect TmrID     : --
  Session Init TmrID       : --                   Session WTR TmrID        : --
  Session Echo Tx TmrID    : -
  PDT Index                : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description      : --
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

说明 以上输出中的“**Process PST : Disable**”表示没有通过 **process-pst** 命令使能系统在 BFD 会话状态变化时修改端口状态表 PST 功能。如果允许 BFD 修改端口状态表 PST（Port State Table），当检测到 BFD 会话状态变为 Down 时，系统将更改 PST 中相应表项。

然后分别在 RouterA 和 RouterB 上配置 BFD 状态与接口状态联动。

```
[RouterA] bfd atob
[RouterA-bfd-session-atob] process-interface-status
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
[RouterB] bfd btoa
[RouterB-bfd-session-btoa] process-interface-status
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置好后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到 BFD Session（BFD 会话）状态为 Up，“Proc interface status”字段显示为“Enable”，表明已配置 **process-interface-status** 命令。以下是 RouterA 上的输出示例。

```
[RouterA] display bfd session all verbose
--------------------------------------------------------------------------------
  Session MIndex : 16384        (One Hop) State : Up          Name : atob
--------------------------------------------------------------------------------
  Local Discriminator      : 10                 Remote Discriminator     : 20
  Session Detect Mode      : Asynchronous Mode Without Echo Function
  BFD Bind Type            : Interface(GigabitEthernet1/0/0)
  Bind Session Type        : Static
  Bind Peer Ip Address     : 224.0.0.184
  NextHop Ip Address       : 224.0.0.184
  Bind Interface           : GigabitEthernet1/0/0
  FSM Board Id             : 3                  TOS-EXP                  : 7
  Min Tx Interval (ms)     : 10                 Min Rx Interval (ms)     : 10
  Actual Tx Interval (ms): 10                   Actual Rx Interval (ms): 10
  Local Detect Multi       : 3                  Detect Interval (ms)     : 30
  Echo Passive             : Disable            Acl Number               : --
  Destination Port         : 3784               TTL                      : 255
  Proc interface status    : Enable             Process PST              : Disable
  WTR Interval (ms)        : 300000
  Active Multi             : 3
  Last Local Diagnostic    : No Diagnostic
  Bind Application         : No Application Bind
  Session TX TmrID         : --                 Session Detect TmrID     : --
  Session Init TmrID       : --                 Session WTR TmrID        : --
  Session Echo Tx TmrID    : -
  PDT Index                : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description      : --
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

对 RouterB 的 GE1/0/1 接口执行 **shutdown** 操作，模拟二层传输设备故障，BFD 会话的状态变为 Down。然后在 RouterA 上执行 **display bfd session all verbose** 命令和 **display interface gigabitethernet 1/0/0** 命令，可以看到 BFD Session（BFD 会话）状态为 Down，但 GE1/0/0 接口的状态仍为 UP。输出示例略。

7.4.5 单臂回声功能配置示例

本示例的基本拓扑结构如图 7-17 所示，RouterA 和 RouterB 通过直连链路连通，RouterA 支持 BFD 功能，RouterB 不支持 BFD 功能。用户希望实现对链路故障的快速检测。

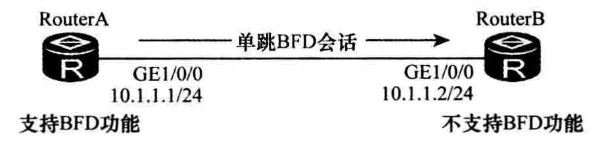


图 7-17 单臂回声功能配置示例拓扑结构

本示例很简单，仅需在 RouterA 上配置单臂回声功能 BFD 会话，就可以实现检测 RouterA 到 RouterB 的直连链路。但要注意的是，**单臂回声功能仅适用于单跳检测功能，而且必须是在通过三层接口直接相连的两台设备间使用。**

根据 7.3.4 小节介绍的配置方法可以很容易得出本示例如下所示的具体配置步骤。

① 配置 RouterA 的接口 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

② 配置 RouterB 的接口 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

③ 配置 RouerA 上的单臂回声 BFD 会话。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 10.1.1.2 interface gigabitEthernet1/0/0 one-arm-echo
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] min-echo-rx-interval 100
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

配置完成后，在 RouterA 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳的 BFD 会话，且状态为 Up，表示单臂回声 BFD 会话建立成功。

```
<RouterA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 256          (One Hop) State : Up          Name : atob
--------------------------------------------------------------------------------
  Local Discriminator     : 1                   Remote Discriminator     : -
  Session Detect Mode     : Asynchronous One-arm-echo Mode
  BFD Bind Type           : Interface(GigabitEthernet1/0/0)
  Bind Session Type       : Static
  Bind Peer IP Address    : 10.1.1.2
  NextHop Ip Address      : 10.1.1.2
  Bind Interface          : GigabitEthernet1/0/0
```

```
FSM Board Id              : 0                    TOS-EXP                  : 7
Echo Rx Interval (ms)     : 100
Actual Tx Interval (ms): 1000                Actual Rx Interval (ms): 1000
Local Detect Multi        : 3                  Detect Interval (ms)     : 3000
Echo Passive              : Disable            Acl Number               : -
Destination Port          : 3784               TTL                      : 255
Proc Interface Status     : Disable            Process PST              : Disable
WTR Interval (ms)         : -
Active Multi              : 3                  Echo Rx Interval(ms)     : 10
Last Local Diagnostic     : No Diagnostic
Bind Application          : No Application Bind
Session TX TmrID          : 87                 Session Detect TmrID     : 88
Session Init TmrID        : -                  Session WTR TmrID        : -
Session Echo Tx TmrID     : -
PDT Index                 : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description       : -
--------------------------------------------------------------------------

    Total UP/DOWN Session Number : 1/0
```

7.5 NQA 配置与管理

随着 Internet 的高速发展，网络支持的业务和应用日渐增多，传统的网络性能分析方法（如 Ping、Tracert 等）已经不能满足用户对业务多样性和监测实时性的要求。NQA（Network Quality Analysis，网络质量分析）是系统提供的一个特性，位于链路层之上，覆盖网络层、传输层和应用层，独立于底层硬件，可实时监视网络性能状况，在网络发生故障时进行故障诊断和定位。

7.5.1 NQA 综述

NQA 通过发送测试报文，对网络性能或服务质量进行分析，为用户提供网络性能参数。它可监测网络上运行的多种协议的性能，使用户能够实时采集到各种网络运行指标，例如 HTTP 的总时延、TCP 连接时延、DNS 解析时延、文件传输速率、FTP 连接时延、DNS 解析错误率等。通过对 NQA 测试结果的分析，用户可以及时了解网络的性能状况，针对不同的网络性能，进行相应的处理；对网络故障进行诊断和定位。

在 NQA 测试中，把测试两端称为客户端和服务器端（或者称为源端和目的端），并由客户端（源端）发起测试。在客户端通过命令行配置测试例或由网管端发送相应测试例操作后，NQA 把相应的测试例放入测试例队列中进行调度。

启动 NQA 测试例，可以选择立即启动、延迟启动、定时启动。在定时器的时间到达后，则根据测试例的测试类型，构造符合相应协议的报文。但配置的测试报文的大小如果无法满足发送本协议报文的最小尺寸，则按照本协议规定的最小报文尺寸来构造报文发送。

测试例启动后，根据返回的报文，可以对相关协议的运行状态提供数据信息。发送报文时的时间作为测试报文的发送时间，并给报文打上时间戳，再发送给服务器端。服

务器端接收报文后，返回给客户端相应的回应信息，客户端在接收到报文时，再一次读取系统的时间，给报文加上时间戳。根据报文的发送和接收时间，计算出报文的往返时间。

AR G3 系列路由器中支持的 NQA 测试例包括 DHCP 测试、DNS 测试、FTP 测试、HTTP 测试、ICMP 测试、SNMP 测试、TCP 测试、Trace 测试、UDP 测试、UDP Jitter 测试、基于接口板发包的 UDP Jitter 测试、LSP Ping 测试和 LSP Trace 测试。其中，ICMP 测试、Trace 测试和 UDP Jitter 测试支持 IPv6 网络，但 AR150/150-S/160/200/200-S 系列不支持 LSP Ping 测试和 LSP Trace 测试。本章仅介绍最常用的 ICMP 测试，至于其他测试原理大家可以到官网上查看相关文档。

说明　对于 Jitter 测试例，不仅客户端需要给报文加时间戳，而且服务器端在接收到报文和发送报文时，也要读取自己的本地系统时间，再加上时间戳，从而能够计算出抖动时间。这样用户就可以通过查看测试数据信息了解网络的运行情况和服务质量。

NQA 还提供了与 Track 和应用模块联动的功能，实时监控网络状态的变化，及时进行相应的处理，从而避免通信的中断或服务质量的降低。目前，NQA 实现了与 VRRP、静态路由、备份接口和策略路由的联动。

7.5.2　ICMP NQA 测试基本原理

NQA 的 ICMP 测试例用于检测源端到目的端的路由是否可达，可以与许多其他功能进行联动，如本书后面将要介绍的 VRRP、静态路由、备份接口和策略路由等。ICMP 测试提供类似于普通命令行下的 Ping 命令功能，但输出信息更为丰富。默认情况下能够保存最近 5 次的测试结果。结果中能够显示平均时延、丢包率、最后一个报文正确接收的时间等信息。

如图 7-18 所示，ICMP 测试的过程如下。

① 源端（RouterA）端向目的端（RouterB）发送构造的 ICMP Echo Request 报文。

② 目的端（RouterB）在收到报文后，直接回应 ICMP Echo Reply 报文给源端（RouterA）。

Network
RouterA
RouterB

图 7-18　ICMP 测试示例

③ 源端（RouterA）收到报文后，通过计算源端（RouterA）接收时间和源端（RouterA）发送时间差，计算出源端（RouterA）到目的端（RouterB）的通信时间，从而清晰地反应出网络性能。如果没有收到 ICMP Echo Reply 报文则表示目的端不可达，可以据此判断监测的链路出现了故障，可通告对应功能模块及时作出相应的处理，如进行备份链路的切换，备份路由的启用。

ICMP 测试的结果和历史记录将记录在测试例中，可以通过命令行来查看探测结果和历史记录。具体将在本章后面介绍。

7.5.3　配置 ICMP NQA 测试

在配置 ICMP 测试之前，需要 NQA 客户端与被测试设备间路由可达。然后在

NQA 客户端进行如表 7-7 所示配置。ICMP NQA 测试的基本配置思想包括三个方面：一是创建一个 NAQ 测试例，然后配置测试例类型为 ICMP，最后配置测试例的 IP 地址。至于其他一些测试参数，因为都有对应的缺省值，所以可根据实际需要选择配置。

表 7-7 **ICMP 测试配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**nqa test-instance** *admin-name test-name* 例如：[Huawei] **nqa test-instance** user test	创建 NQA 测试例，并进入 NQA 测试例视图。命令中的参数说明如下 ● *admin-name*：创建进行 NQA 测试的管理员账户，1～32 个字符，不支持空格，区分大小写 ● *test-name*：配置 NQA 测试例的测试例名称，1～32 个字符，不支持空格，区分大小写 缺省情况下，没有创建 NQA 测试例，可用 **undo nqa** { **test-instance** *admin-name test-name* | **all-test-instance** } 命令删除指定或所有的 NQA 测试例
3	**test-type icmp** 例如：[Huawei-nqa-user-test] **test-type icmp**	配置以上创建的 NQA 测试例的类型为 ICMP NQA 测试例 缺省情况下，未配置任何测试类型，可用 **undo test-type** 命令删除 NQA 测试例的测试类型的配置
4	**destination-address ipv4** *ipv4-address*t 例如：[Huawei-nqa-user-test] **destination-address ipv4** 1.1.1.1	（可选）配置 NQA 测试例的目的 IPv4 地址 缺省情况下，没有配置目的地址，可用 **undo destination-address** 命令删除对应 NQA 测试例的目的 IPv4 地址
5	**description** *string* 例如：[Huawei-nqa-user-test] **description** icmp	（可选）配置 NQA 测试例的描述信息，取值范围为 1～230 个字符，支持空格，区分大小写 缺省情况下，NQA 测试例没有配置描述信息，可用 **undo description** 命令删除以上 NQA 测试例的描述信息 【注意】本命令为覆盖型命令，以最后一次配置为准，且不能修改正在执行的测试例的描述信息
6	**frequency** *interval* 例如：[Huawei-nqa-user-test] **frequency** 20	（可选）配置 NQA 测试例自动执行测试的时间间隔，取值范围为 1～604 800 的整数秒。**但取值必须大于下面第 16 步 interval 和第 14 步 probe-count 两命令的配置值的乘积** 缺省情况下，没有配置自动测试间隔，即只进行一次测试，可用 **undo frequency** 命令取消配置的 NQA 测试例自动执行测试的时间间隔
7	**timeout** *time* 例如：[Huawei-nqa-user-test] **timeout** 20	（可选）配置 NQA 测试例的一次探测的超时时间，取值范围为 1～60 的整数秒。如果超过此时间没有收到响应报文，认为该次测试失败。对于质量较差、传输速率不高的网络，为了保证 NQA 探测报文能够收到回应，需要加大发送探测报文的超时时间 缺省情况下，超时时间为 3 s，可用 **undo timeout** 命令恢复 NQA 测试例的一次探测的超时时间的缺省值

（续表）

步骤	命令	说明
8	**source-interface** *interface-type interface-number* 例如：[Huawei-nqa-user-test] **source-interface** gigabitethernet 1/0/0	（可选）配置 NQA 测试例的源端接口（**必须是已经配置了 IP 地址的接口**） 【说明】如果通过下面第 9 步的 **source-address** 命令指定 NQA 测试例的源 IP 地址，并且通过本命令指定了 NQA 测试例的源接端口，则报文会从指定源接口发送出去，但是回应报文会从配置的源 IP 地址的接口返回；如果没有指定 NQA 测试例的源 IP 地址，而通过本命令指定了源端接口，则 NQA 测试例将使用指定的源端接口的 IP 地址作为 NQA 测试例的源 IP 地址，但 NQA 测试例的发送和回应报文都会“走”本命令指定的源接口 缺省情况下，没有配置 NQA 测试例的源端接口，可用 **undo source-interface** 命令取消 NQA 测试例的源端接口配置
9	**source-address ipv4** *ipv4-address* 例如：[Huawei-nqa-user-test] **source-address ipv4** 1.1.1.1	（可选）配置 NQA 测试的源端的 IPv4 地址，相当于 **ping** 命令中的“**-a**”选项 【说明】当测试报文到达目的地址后，会将 NQA 测试例配置的源 IP 地址作为目的地址进行回应。执行本命令配置本次测试的源 IP 地址。若不指定源 IP 地址，系统将使用发送测试报文的接口 IP 地址作为源 IP 地址 缺省情况下，使用发送测试报文的接口 IP 地址作为源 IP 地址，可用 **undo source-address** 命令恢复 NQA 测试的源端的 IP 地址为缺省情况
10	**ttl** *number* 例如：[Huawei-nqa-user-test] **ttl** 10	（可选）配置 NQA 测试例测试报文的 TTL 值，相当于 **ping** 命令中的“**-h**”选项，取值范围为 1～255 的整数 【说明】在最初创建测试报文时，**ttl** 命令设置 TTL 为某个特定的值。当测试报文逐个沿三层路由设备进行传输时，每台三层路由设备都使 TTL 的数值减 1，当 TTL 的值减为 0 时，三层路由设备会丢弃该测试报文并向发送端发送错误信息。从而有效地防止了报文的无休止传输。如果已经配置过 TTL 值，那么再次执行本命令将覆盖原有配置 缺省情况下，TTL 值为 30，可用 **undo ttl** 命令恢复 NQA 测试例测试报文的 TTL 值为缺省值
11	**datasize** *size* 例如：[Huawei-nqa-user-test] **datasize** 100	（可选）配置 NQA 测试例的报文数据区大小，相当于 **ping** 命令中的“-s”选项，实现模拟实际业务数据包大小，得到更加精确的统计数据，取值范围为 0～8 100 整数个字节。如果配置的报文大小比报文默认长度小，实际的报文大小就按默认报文长度处理 缺省情况下，NQA 测试例数据区大小为 0，表示不携带负载报文，可用 **undo datasize** 命令恢复 NQA 测试例的报文大小为缺省值
12	**datafill** *fillstring* 例如：[Huawei-nqa-user-test] **datafill** abcd	（可选）配置 NQA 测试例的填充字符（用于实现对测试报文的标识，区分不同的测试例发出的报文），相当于 **ping** 命令中的“**-p**”选项，取值范围为 1～230 个字符，支持空格，区分大小写，支持特殊字符，但必须小于等于 **datasize** *size* 命令配置的数据区大小 缺省值是空字符串（长度为零），可用 **undo datafill** 命令删除 NQA 测试例的填充字符

（续表）

步骤	命令	说明
13	**sendpacket passroute** 例如：[Huawei-nqa-user-test] **sendpacket passroute**	（可选）配置 NQA 测试例不查找路由表发送报文，但此时会造成同时配置的 **ttl** 或 **ip-forwarding** 命令无效。 缺省情况下，NQA 测试查找路由表发送报文，可用 **undo sendpacket passroute** 命令恢复 NQA 测试例查找路由表发送报文
14	**probe-count** *number* 例如：[Huawei-nqa-user-test] **probe-count** 6	（可选）配置 NQA 测试例的一次测试探针数目，取值范围为 1～15 的整数。**对于不可靠网络，可将探测次数取值设置相对大些，因为可能发送较大次数的探测报文才能获得探测成功** 缺省情况下，一次测试探针数目是 3，可用 **undo probe-count** 命令恢复 NQA 测试例的一次测试探针数目为缺省值
15	**tos** *value* 例如：[Huawei-nqa-user-test] **tos** 10	（可选）配置 NQA 测试报文的服务类型（通过配置 ToS 值，可以设置探测报文的优先级别（数值越大，优先级越高），在报文流量较大时可以先处理优先级高的报文），相当于 **ping** 命令中的"**-tos**"选项，取值范围为 0～255 的整数 缺省情况下，ToS 的值为 0，可用 **undo tos** 命令恢复 NQA 测试报文的服务类型为缺省值
16	**fail-percent** *percent* 例如：[Huawei-nqa-user-test] **fail-percent** 10	（可选）配置 NQA 测试失败百分比，用来判断某次测试是否失败，即如果发送探测包失败的次数超过该比值，则认为该次测试失败，取值范围为 1～100 的整数 缺省情况下，测试失败百分比为 100%，即只有全部探测失败，本次测试才视为失败，可用 **undo fail-percent** 命令删除 NQA 测试失败百分比配置
17	**interval seconds** *interval* 例如：[Huawei-nqa-user-test] **interval** 30	（可选）配置测试报文的发送间隔，相当于 **ping** 命令中的"**-m**"选项，取值范围为 1～60 的整数秒，**但必须大于本表第 7 步配置的一次探测的超时时间** 缺省情况下，ICMP 测试例发送报文的时间间隔为 4 s，可用 **undo interval** 命令恢复 NQA 测试例的发送报文的时间间隔为缺省值
18	**vpn-instance** *vpn-instance-name*	（可选）配置 NQA 测试例的 VPN 实例名，1～31 个字符 缺省情况下，未配置 VPN 实例名，可用 **undo vpn-instance** 命令删除 NQA 测试例的 VPN 实例名
19	**records history** *number* 例如：[Huawei-nqa-user-test] **records history** 30	（可选）配置 NQA 测试的最大历史记录数目，取值范围为 1～50 的整数 缺省情况下，历史记录为 50，可用 **undo records** history 命令恢复 NQA 测试的历史记录最大数目为缺省值
20	**records result** *number* 例如：[Huawei-nqa-user-test] **records result** 5	（可选）配置 NQA 测试的最大测试结果记录数目，取值范围为 1～10 的整数 缺省情况下，结果记录数为 5，可用 **undo records result** 命令恢复 NQA 测试的结果记录的最大数目为缺省值
21	**agetime** *hh:mm:ss* 例如：[Huawei-nqa-user-test] **agetime** 1:0:0	（可选）配置 NQA 测试例的老化时间（改变测试例在系统中存在的时间），*hh* 用来指定小时数，取值范围为 0～23 的整数，*mm* 用来指定分钟数，取值范围为 0～59 的整数，*ss* 用来指定秒数，取值范围为 0～59 的整数 缺省情况下，老化时间为 0，表示测试例永不老化，可用 **undo agetime** 命令恢复 NQA 测试例老化时间为缺省值

（续表）

<table>
<tr><th>步骤</th><th>命令</th><th colspan="2">说明</th></tr>
<tr><td>22</td><td>ip-forwarding
例如：[Huawei-nqa-user-test] ip-forwarding</td><td colspan="2">（可选）配置头节点强制走 IP 转发。但是在 MPLS 网络中，当 MPLS 网络故障且控制层面无法正常感知时，会出现 ping 不通的情况，指定 ping 头节点强制走 IP 转发，区分是 MPLS 网络问题还是 IP 网络问题，可以帮助用户快速定位故障</td></tr>
<tr><td>23</td><td>nexthop ipv4 ip-address
例如：[Huawei-nqa-user-test] nexthop ipv4 10.1.1.1</td><td colspan="2">（可选）配置测试例的下一跳 IPv4 地址。本命令只有 V2R5 的版本才有
【说明】NQA 联动静态路由场景下，当链路故障时，ICMP NQA 测试例检测结果是失败，同时联动静态路由变为 DOWN。一旦链路故障恢复，由于 ICMP 测试例报文发送时需要查找路由表，但此时路由已经被 NQA 联动置 DOWN，导致 ICMP 测试例仍然检测失败，联动的静态路由也一直得不到恢复，业务流量也无法回切到原先的链路。解决方案是指定 ICMP 测试例发送报文时的下一跳地址，这样在链路故障恢复之后可以正常发送 NQA 探测报文，测试结果恢复成功，同时可联动恢复静态路由
配置测试的下一跳地址后，测试例报文发送时将不再查找路由表，而是直接按指定的下一跳地址发送。但指定的下一跳地址和出接口相互匹配，且指定的出接口不能是逻辑接口的成员接口；指定下一跳地址时，不支持同时在本表第 17 步中指定 VPN
缺省情况下，查找路由表获取下一跳地址，可用 undo nexthop 命令删除配置的 NQA 测试的下一跳地址</td></tr>
<tr><td rowspan="3">24</td><td>start now [end { at [yyyy/mm/dd] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }]
例如：[Huawei-nqa-user-test] start delay 10:00:00</td><td>（三选一）立即启动 NQA 测试例</td><td rowspan="3">三个命令中的参数和选项说明如下
• start now：指定立即启动执行当前测试例
• end at [yyyy/mm/dd] hh:mm:ss：二选一参数，在指定的时间点结束当前执行的测试例
• start at [yyyy/mm/dd] hh:mm:ss：二选一参数，指定开始执行测试例的时间
• end delay { seconds second | hh:mm:ss }：二选一参数，指定延迟结束测试例的执行，即从当前执行命令的时间开始算起，一直持续到所设定的延迟时间后才结束。该延迟是相对于当前系统时间的延迟。例如：当用户在 8:59:40 执行命令 start at 9:00:00 end delay seconds 60（从 8:59:40 开始延迟 60 s 后结束）时，测试例在 9:00:00 开始执行，在 9:00:40 结束
• end lifetime { seconds second | hh:mm:ss }：二选一参数，配置测试例的持续时间，但从测试例启动的时间开始算起。例如：当用户在 9:00:00 执行命令 start delay seconds 60 end lifetime seconds 120 时，测试例开始执行时间是 09:01:00，持续时间为 120 s，结束时间是 09:03:00
缺省情况下，测试报文发送完毕后，测试自动结束，可用 undo start 命令终止当前正在执行的测试例或者删除未执行 NQA 测试例的启动方式和结束方式的配置</td></tr>
<tr><td>start at [yyyy/mm/dd] hh:mm:ss [end { at [yyyy/mm/dd] hh:mm:ss | delay { seconds second | hh:mm:ss } |lifetime { seconds second | hh:mm:ss } }]
例如：[Huawei-nqa-user-test]start at 9:00:00</td><td>（三选一）在指定时刻启动 NQA 测试例</td></tr>
<tr><td>start delay { seconds second | hh:mm:ss } [end { at [yyyy/mm/dd] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } }]
例如：[Huawei-nqa-user-test]start delay seconds 60 end lifetime seconds 120</td><td>（三选一）延迟指定时间后启动 NQA 测试例</td></tr>
</table>

（续表）

步骤	命令	说明
25	**restart** 例如：[Huawei-nqa-user-test] **restart**	（可选）重新启动 NQA 测试例。**仅当需要重新启动测试例时才执行本命令**

7.5.4 ICMP NQA 测试管理

完成 ICMP NQA 的测试例配置之后，可通过执行下列 **display** 任意视图命令查看 ICMP NQA 测试例的配置信息，使用以下 **clear** 或者 **reset** NQA 测试例视图命令清除 ICMP 测试例统计信息（但不允许清除正在运行的测试例的统计信息）。

① **display nqa application**：查看 NQA 客户端与业务对应的 NQA 测试例类型。

② **display nqa-parameter**：查看 NQA 客户端当前测试例的参数配置信息。

③ **display nqa support-server-type**：查看 NQA 客户端支持的服务器类型。

④ **display nqa support-test-type**：查看 NQA 客户端支持的测试例类型。

⑤ **display nqa-agent**：查看 NQA 测试的客户端状态和配置信息。

⑥ **display nqa-server**：在 NQA 服务器端查看服务器信息。

⑦ **display nqa results** [**collection** | **success** | **failed**] [**test-instance** *admin-name test-name*]：查看所有或者指定的 NQA 测试例的 NQA 测试结果信息。

⑧ **display nqa history** [**test-instance** *admin-name test-name*] [**from** *start-date start-time* **to** *end-date end-time*]：查看所有或者指定 NQA 测试例的 NQA 测试的历史统计信息。

⑨ **clear-records**：清除 NQA 测试例的统计信息。

⑩ **reset ip nqa-compatible responder statistics**：清除设备收到第三方设备或网管软件发送的 NQA 握手报文的统计信息。

7.5.5 ICMP NQA 测试配置示例

本示例的基本拓扑结构如图 7-19 所示，RouterA 作为 NQA 客户端（Client），现要测试 RouterB（作为 NQA 服务器端）是否可达。

RouterA　GE1/0/0　10.1.1.1/24　NQA Client
RouterB　GE1/0/0　10.1.1.2/24

图 7-19　ICMP NQA 测试配置示例基本拓扑结构

1. 基本配置思路分析

本示例的配置很简单，仅需要使用 ICMP NQA 测试功能，配置一个 ICMP 测试例，测试报文在本端（RouterA）和指定的目的端（RouterB）之间是否可达，可选测试。至于 7.5.3 小节介绍的其他可选配置，在此可不用配置。

2. 具体配置步骤

① 配置 RouterA 和 RouterB 的相关接口 IP 地址。

RouterA 上的配置。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 上的配置。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

② 在 RouterA 上使能 NQA 客户端，配置一个名为 icmp，管理者账户为 admin 的 ICMP 类型的 NQA 测试例。

```
[RouterA] nqa test-instance admin icmp
[RouterA-nqa-admin-icmp] test-type icmp
[RouterA-nqa-admin-icmp] destination-address ipv4 10.1.1.2
```

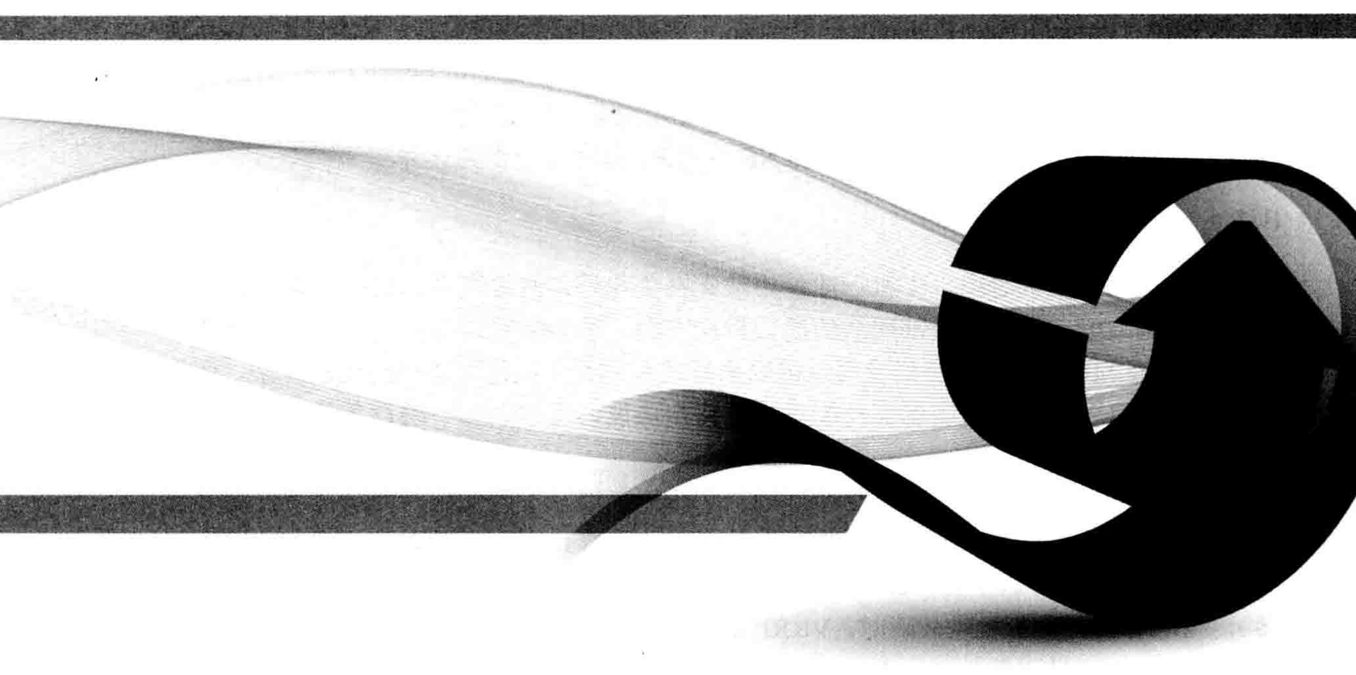
③ 立即启动测试。

```
[RouterA-nqa-admin-icmp] start now
```

配置好后要，可用 **display nqa results** 命令查看测试结果，验证配置是否正确。

```
[RouterA-nqa-admin-icmp] display nqa results test-instance admin icmp
 NQA entry(admin, icmp) :testflag is inactive, testtype is icmp
  1 . Test 1 result     The test is finished
   Send operation times: 3                       Receive response times: 3
   Completion:success                             RTD OverThresholds number: 0
   Attempts number:1                              Drop operation number:0
   Disconnect operation number:0                 Operation timeout number:0
   System busy operation number:0                Connection fail number:0
   Operation sequence errors number:0           RTT Stats errors number:0
   Destination ip address:10.1.1.2
   Min/Max/Average Completion Time: 31/46/36
   Sum/Square-Sum   Completion Time: 108/4038
   Last Good Probe Time: 2012-8-2 10:7:11.4
   Lost packet ratio: 0 %
```

第8章 VRRP配置与管理



VRRP（虚拟路由冗余协议）就是指将多个路由设备（可以是路由器，也可以是三层交换机）组成一台虚拟路由设备，并在其中指定一台成员路由设备作为主用（Master）设备，其他成员设备作为主用设备不可用时的备用（Backup）设备，然后为这台虚拟路由器分配一个IP地址，作为下游设备的默认网关，这样就可防止单点故障问题，实现路由设备容错，为上、下游设备保持持续的连通服务。VRRP除了最基本的主备备份功能外，还可通过配置多个虚拟备份组，指定不同设备担当主用设备，实现多路由设备之间的负载分担；还可与各种其他对象一起联动，实现更加强大的监视功能。

本章介绍的是AR G3系列路由器中的VRRP功能配置与管理方法。总体而言，VRRP的配置很简单，最基本的功能只需创建所需的VRRP备份组，并为之配置虚拟路由器IP地址，为Master设备配置更高的优先级，就可以实现主备备份。通过创建多个以不同设备作为Master设备的VRRP备份组就可实现不同路由设备间的负载分担。至于其他一些可选项或者参数大多数情况下是无需配置的，直接采用它们的缺省配置即可。本章内容的另一个重点就是VRRP与其他对象的联动配置（如与接口状态联动、与BFD/NQA/路由的联动等），以解决基本VRRP功能的某些不足。本章实例丰富，充分考虑到了VRPP各主要应用环境，读者可直接拿来即用。

注意 VRRP有支持IPv4的v2版本以及同时支持IPv4和IPv6的v3版本，但本书仅介绍支持IPv4的v2版本。

8.1 VRRP 基础

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种容错协议，可通过把几台路由设备联合组成一台虚拟的路由设备，然后使用一定的机制保证在下一跳路由设备出现故障时上一跳设备及时将业务切换到备份路由设备，从而保持通信的连续性和可靠性。VRRP 在华为 S 系列三层交换机、AR G3/NE 系列路由器中都可得到应用。

8.1.1 VRRP 概述

在一般的网络部署中，主机一般使用缺省网关与外部网络联系，这样一来，如果缺省网关发生故障，主机与外部网络的通信将被中断。虽然配置动态路由协议（如 RIP、OSPF）或 ICMP 路由发现协议等可以提高系统的可靠性，但是配置过程比较复杂，而且并不能保证每台上一跳设备都支持配置动态路由协议，比如，上一跳设备是用户主机或者二层交换机就不支持。

VRRP 的出现很好地解决了这个问题。VRRP 能够在不改变组网的情况下，将多台路由设备组成一个虚拟路由器，通过配置虚拟路由器的 IP 地址作为缺省网关，实现对缺省网关的备份（因为这个虚拟路由器的 IP 地址可代表整个虚拟路由器中各个成员路由设备）。当现有网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

如图 8-1 所示，HostA 通过 SwitchA 双线连接到 RouterA 和 RouterB。现在 RouterA 和 RouterB 上配置 VRRP 备份组，对外体现为一台虚拟路由器，实现到达 Internet 的链路冗余备份。

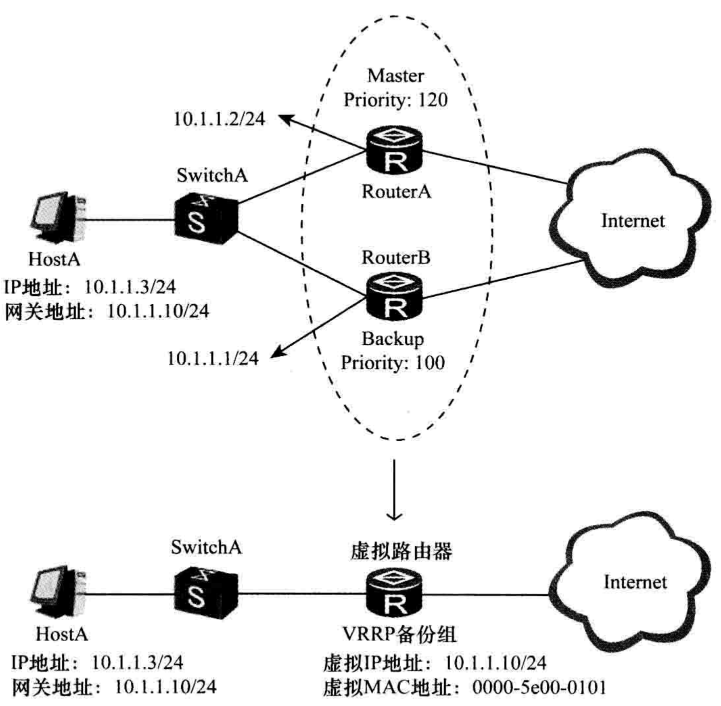


图 8-1　VRRP 备份组形成示意图

1. 基本概念

因为在后面正式介绍 VRRP 工作原理和配置过程中会遇到许多与 VRRP 相关的基本概念，所以在此先介绍这些 VRRP 基本概念。

① VRRP 路由器（VRRP Router）：运行 VRRP 的设备（可以是路由器，也可以是三层交换机，下同），**可加入到一个或多个虚拟路由器备份组中。**

② 虚拟路由器（Virtual Router）：又称 VRRP 备份组，**由一个 Master（主用）设备和多个 Backup（备用）设备组成**，被当作一个共享局域网内主机的缺省网关。

③ Master 路由器（主用路由器）：VRRP 备份组中当前承担转发报文任务的 VRRP 设备。

④ Backup 路由器（备用路由器）：VRRP 备份组中一组没有承担转发任务的 VRRP 设备，但当 Master 设备出现故障时，它们将可通过选举成为新的 Master 设备。

⑤ VRID：虚拟路由器标识，用来唯一标识一个 VRRP 备份组。

⑥ 虚拟 IP 地址（Virtual IP Address）：分配给虚拟路由器的 IP 地址。一个虚拟路由器可以有一个或多个 IP 地址（多个 IP 地址时，只有一个是主 IP 地址，其他为从 IP 地址），由用户配置。

⑦ IP 地址拥有者（IP Address Owner）：如果一个 VRRP 设备将虚拟路由器的 IP 地址作为真实的接口地址，则该设备被称为 IP 地址拥有者。**如果该 IP 地址拥有者是可用的，将直接成为 Master，不用选举，也不可抢占**，除非该设备不可用。

⑧ 虚拟 MAC 地址（Virtual MAC Address）：是虚拟路由器根据虚拟路由器 ID（VRID）生成的 MAC 地址。一个虚拟路由器拥有一个虚拟 MAC 地址，格式为：00-00-5E-00-01-{*VRID*}。当虚拟路由器回应 ARP 请求时，使用的是虚拟 MAC 地址，而不是接口的真实 MAC 地址。

⑨ 优先级（Priority）：用来标识虚拟路由器中各成员路由设备的优先级。虚拟路由器根据优先级选举出 Master 设备和 Backup 设备。

⑩ 抢占模式：在抢占模式下，如果 Backup 设备的优先级比当前 Master 设备的优先级高，则主动将自己切换成 Master。

⑪ 非抢占模式：在非抢占模式下，只要 Master 设备没有出现故障，Backup 设备即使随后被配置了更高的优先级也不会成为 Master 设备。

2. VRRP 的主要好处

配置 VRRP 功能，可以带来以下好处。

① 简化网络管理：VRRP 能在当前网关设备出现故障时仍然提供高可靠的缺省链路，且无需修改动态路由协议、路由发现协议等配置信息，可有效避免单一链路发生故障后的网络中断问题。

② 适应性强：VRRP 报文封装在 IP 报文中，支持各种上层协议。

③ 网络开销小：VRRP 只定义了一种报文，即 VRRP 协议报文，有效减轻了网络设备的额外负担。

8.1.2 VRRP 协议报文

要理解 VRRP 协议的工作原理，先要了解 VRRP 协议报文。VRRP 协议报文是用来

将 Master 设备的优先级和状态通告给同一备份组的所有 Backup 设备，**即仅 Master 设备会发送 VRRP 协议报文**。它们封装在 IP 报文中，通过 VRRP 组播 IP 地址进行发送，报文头中源地址为发送报文接口的主 IP 地址（不是虚拟路由器的 IP 地址），目的地址为 VRRP 组播 IP 地址 224.0.0.18，TTL 是 255，协议号是 112。

目前，VRRP 协议包括两个版本：VRRPv2 和 VRRPv3。VRRPv2 仅适用于 IPv4 网路，VRRPv3 适用于 IPv4 和 IPv6 两种网络。基于不同的网络类型，VRRP 可以分为 VRRP for IPv4 和 VRRP for IPv6（简称 VRRP6）。VRRP for IPv4 支持 VRRPv2 和 VRRPv3，而 VRRP for IPv6 仅支持 VRRPv3。**本章仅介绍针对 IPv4 网络的 VRRP 应用配置。**

VRRPv2 和 VRRPv3 的报文结构分别如图 8-2 和图 8-3 所示，各字段说明如表 8-1 所示。

0　　3	4　　7	15	23	31
Version	Type	Virtual Rtr ID	Priority	Count IP Addrs
Auth Type		Adver Int	Checksum	
IP Address (1)				
⋮				
IP Address (n)				
Authentication Data (1)				
Authentication Data (2)				

图 8-2　VRRPv2 报文结构

0　　3	4　　7	8　　15	16　　23	24　　31
Version	Type	Virtual Rtr ID	Priority	Count IPvX Addr
(rsvd)	Max Adver Int		Checksum	
IPvX Address (es)				

图 8-3　VRRPv3 报文结构

表 8-1　VRRPv2 和 VRRPv3 报文字段说明

报文字段	说明	
	VRRPv2	VRRPv3
Version	VRRP 协议版本号，取值为 2	VRRP 协议版本号，取值为 3
Type	VRRP 报文类型，取值为 1，表示 Advertisement（通告）类型	
Virtual Rtr ID（VRID）	虚拟路由器 ID，取值范围为 1～255	

（续表）

报文字段	说明	
	VRRPv2	VRRPv3
Priority	表示 Master 设备在备份组中的优先级，取值范围是 0～255。0 表示设备要停止参与 VRRP 备份组，用来使备份设备尽快成为 Master 设备，而不必等到计时器超时；255 则保留给虚拟路由器 IP 地址的拥有者。缺省值是 100	
Count IP Addrs/ Count IPvX Addr	表示 VRRP 备份组中虚拟 IPv4 地址的个数	表示 VRRP 备份组中虚拟 IPv4 或虚拟 IPv6 地址的个数
Auth Type	VRRP 报文的认证类型。协议中指定了以下 3 种类型 • 0：Non Authentication，表示不进行认证 • 1：Simple Text Password，表示采用明文密码认证方式 • 2：IP Authentication Header，表示采用 MD5 认证方式	无此字段
Adver Int/Max Adver Int	表示 VRRP 通告报文的发送时间间隔，单位是秒，缺省值为 1 s	表示 VRRP 通告报文的发送时间间隔，单位是厘秒，缺省值为 100 厘秒
Checksum	16 位校验和，用于检测 VRRP 报文中的数据破坏情况	
IP Address/IPvX Address(es)	表示 VRRP 备份组的虚拟 IPv4 地址，所包含的地址数定义在 Count IP Addrs 字段	表示 VRRP 备份组的虚拟 IPv4 地址或者虚拟 IPv6 地址，所包含的地址数定义在 Count IPvX Addrs 字段
Authentication Data	表示认证数据。目前只有明文密码认证和 MD5 认证才用到该部分，对于其他认证方式，一律填 0	无此字段
rsvd	无此字段	VRRP 报文的保留字段，必须设置为 0

由以上 VRRPv2 和 VRRPv3 的报文结构可以看出，两者的主要区别如下。

① 支持的网络类型不同。VRRPv3 适用于 IPv4 和 IPv6 两种网络，而 VRRPv2 仅适用于 IPv4 网络。

② 认证功能不同。VRRPv3 不支持认证功能，而 VRRPv2 支持认证功能，那是因为 IPv6 协议已有自己的认证功能，IPSec 是 IPv6 的必备组成部分。

③ 发送通告报文的时间间隔的单位不同。VRRPv3 支持的是厘秒级（发送频率更高），而 VRRPv2 支持的是秒级。

8.1.3 VRRP 基本工作原理

VRRP 的工作原理主要体现在设备的协议状态改变上。在 VRRP 中定义了三种状态机：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中，只有处于 Master 状态的设备才可以转发发送到虚拟路由器 IP 地址的数据报文。这三种协议状态之间的转换关系如图 8-4 所示，具体说明如表 8-2 所示。

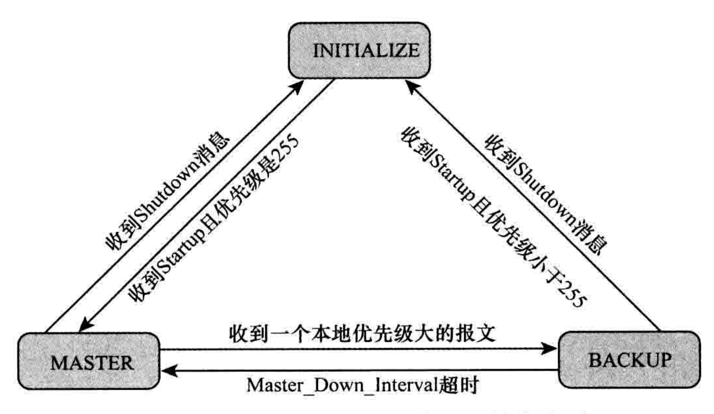


图 8-4 VRRP 三种状态机之间的转换关系

表 8-2 VRRP 协议的三种状态及相互转换关系

状态	说明
Initialize	初始状态，为 VRRP 不可用状态，在此状态时设备不会对 VRRP 报文做任何处理。通常刚配置 VRRP 时或设备检测到故障时会进入该状态 收到接口 Startup（启动）的消息后，如果设备的优先级为 255（表示该设备为虚拟路由器 IP 地址拥有者），则直接成为 Master 设备，如果设备的优先级小于 255，则会先切换至 Backup 状态
Master	活动状态，表示当前设备为 Master 设备。当 VRRP 设备处于 Master 状态时，该设备会做下列工作 ● 定时发送 VRRP 通告报文 ● 以虚拟 MAC 地址响应对虚拟 IP 地址的 ARP 请求 ● 转发目的 MAC 地址为虚拟 MAC 地址的 IP 报文 ● 如果它是这个虚拟 IP 地址的拥有者，则接收目的 IP 地址为这个虚拟 IP 地址的 IP 报文；否则，丢弃这个 IP 报文 ● 如果收到比自己优先级大的 VRRP 报文，或者收到与自己优先级相等的 VRRP 报文，且本地接口 IP 地址小于源端接口 IP 地址时，则立即转变为 Backup 状态（**仅在抢占模式下生效**） ● 收到接口 Shutdown（关闭）消息后，则立即转变为 Initialize 状态
Backup	备份状态，表示当前设备为 Backup 设备。当 VRRP 设备处于 Backup 状态时，该设备将会做下列工作。 ● 接收 Master 设备发送的 VRRP 通告报文，判断 Master 设备的状态是否正常 ● 对虚拟路由器 IP 地址的 ARP 请求不做响应 ● 丢弃目的 MAC 地址为虚拟路由器 MAC 地址的 IP 报文 ● 丢弃目的 IP 地址为虚拟路由器 IP 地址的 IP 报文 ● 如果收到优先级和自己相同，或者比自己高的 VRRP 报文，则重置 Master_Down_Interval 定时器（不进一步比较 IP 地址） 【说明】Master_Down_Interval 定时器是用来确定 Master 设备是否工作正常的定时器。Backup 设备在该定时器超时后仍未收到 Master 设备发来的 VRRP 通告报文时，就会直接转换为 Master 状态。计算公式如下：Master_Down_Interval=(3* Advertisement_Interval) + Skew_time。其中，Skew_Time=(256–Priority)/256 ● 如果收到比自己优先级小的 VRRP 报文，且该报文优先级是 0（表示发送 VRRP 报文的原 Master 设备声明不再参与 VRRP 组了）时，定时器时间设置为 Skew_time（偏移时间） ● 如果收到比自己优先级小的 VRRP 报文，且该报文优先级不是 0，则丢弃报文，立刻转变为 Master 状态（**仅在抢占模式下生效**） ● 如果 Master_Down_Interval 定时器超时，则立即转变为 Master 状态 ● 如果收到接口 Shutdown 消息，则立即转变为 Initialize 状态

总体来说，VRRP 的基本工作原理如下。

① VRRP 备份组中的设备根据优先级选举出 Master，具体选举规则将在下节介绍。选举后的 Master 设备会通过发送免费 ARP 报文，将虚拟 MAC 地址通知给与它连接的设备或者主机，以便在这些设备上建立到达虚拟路由器的 ARP 映射表，发送报文到虚拟路由器。同时，Master 设备又会周期性地向备份组内所有 Backup 设备发送 VRRP 通告报文，以公布其配置信息（优先级等）和工作状况。

② 如果当前 Master 设备出现故障，将在 Master_Down_Interval 定时器超时后，或者由其他联动技术（如与 BFD 的联动）检测到 Master 设备故障后，VRRP 备份组中的 Backup 设备根据优先级重新选举新的 Master。如果备份组中原来就只有两台设备，则原来的 Backup 设备直接转换为 Master 设备。

③ 新的 Master 设备会立即发送携带虚拟路由器的虚拟 MAC 地址和虚拟 IP 地址信息的免费 ARP 报文，刷新与它连接的主机或设备中的 MAC 表项，从而把用户流量引到新的 Master 设备上来，整个过程对用户完全透明（也就不需要用户干预）。

④ 当原 Master 设备故障恢复时，如果该设备为虚拟路由器 IP 地址拥有者（优先级为 255），将直接切换至 Master 状态；否则，将首先切换至 Backup 状态，且其优先级恢复为故障前配置的优先级。

⑤ 如果 Backup 设备设置为抢占方式，则当 Backup 设备的优先级高于当前 Master 设备时，将立即抢占现有 Master 设备，否则仅在当前 Master 设备不可用时 Backup 设备才有可能会成为 Master 设备。

8.1.4 VRRP Master 选举和状态通告

从上节介绍的 VRRP 基本工作原理可以知道，为了保证 Master 设备和 Backup 设备能够协调工作，VRRP 需要实现以下两项基本功能。

① Master 设备的选举。

② Master 设备状态的通告。

下面分别予以介绍。

1. Master 设备的选举

VRRP 根据优先级来确定虚拟路由器中每台设备的角色，Master 设备或 Backup 设备，对应于上节介绍的 Master 状态或 Backup 状态。优先级越高，则越有可能成为 Master 设备。下面是 Master 设备的整个选举过程。

① 初始创建的 VRRP 设备都工作在 Initialize 状态，当 VRRP 设备在收到 VRRP 接口 Startup 的消息后，如果此设备的优先级等于 255（也就是所配置的虚拟路由器 IP 地址是本设备 VRRP 接口的真实 IP 地址），将会直接切换至 Master 状态，**并且无需进行下面的 Master 选举**。否则，会先切换至 Backup 状态，待 Master_Down_Interval 定时器超时后再切换至 Master 状态（因为一开始，还没有最终选举 Master 设备，则这个 Master_Down_Interval 定时器最终肯定会超时）。

② 首先切换至 Master 状态的 VRRP 设备通过 VRRP 通告报文的交互获知虚拟设备中其他成员的优先级，然后根据以下规则进行 Master 的选举。

- 如果收到的 VRRP 报文中显示的 Master 设备的优先级高于或等于自己的优先级，

则当前 Backup 设备保持 Backup 状态。

- 如果 VRRP 报文中 Master 设备的优先级低于自己的优先级，当采用抢占方式时（**缺省为抢占方式**），则当前 Backup 设备将切换至 Master 状态；当采用非抢占方式时，当前 Backup 设备仍保持 Backup 状态。

说明 如果有多个 VRRP 设备同时切换到 Master 状态，通过 VRRP 通告报文的交互进行协商后，优先级较低的 VRRP 设备将切换成 Backup 状态，优先级最高的 VRRP 设备成为最终的 Master 设备；优先级相同时，再根据 VRRP 设备上 VRRP 备份组所在接口主 IP 地址大小进行比较，IP 地址较大的成为 Master 设备。

2. Master 设备状态的通告

Master 设备会周期性地发送 VRRP 通告报文，在 VRRP 备份组中公布其配置信息（优先级等）和工作状况。Backup 设备通过接收到 Master 设备发来的 VRRP 报文的情况来判断 Master 设备是否工作正常。

① 当 Master 设备主动放弃 Master 地位（如 Master 设备退出备份组）时，会发送优先级为 0 的 VRRP 通告报文，使 Backup 设备快速切换成 Master 设备（**当有多台 Backup 设备时也要进行以上介绍的 Master 选举**），而不用等到 Master_Down_Interval 定时器超时。这个切换的时间称为 Skew_time，计算方式为：（256－Backup 设备的优先级）/256，单位为秒。

② 当 Master 设备发生网络故障而不能发送 VRRP 通告报文的时候，Backup 设备并不能立即知道其工作状况，要等到 Master_Down_Interval 定时器超时后，才会认为 Master 设备无法正常工作，从而将状态切换为 Master（**同样，当有多台 Backup 设备时也要进行以上介绍的 Master 选举**）。其中，Master_Down_Interval 定时器取值为：（3×Advertisement_Interval）+Skew_time，单位为秒。

说明 在性能不稳定的网络中，网络堵塞可能导致 Backup 设备在 Master_Down_Interval 定时器超时后仍没有收到 Master 设备的报文后，使得 Backup 设备主动切换为 Master。如果此时原 Master 设备的报文又到达了，新 Master 设备将再次切换回 Backup。如此则会出现 VRRP 备份组成员状态频繁切换的现象。为了缓解这种现象，可以配置抢占延时，使得 Backup 设备在等待了 Master_Down_Interval 定时器后再等待抢占延迟时间（具体将在本章后面介绍）。如果在此期间仍没有收到通告报文，Backup 设备才会切换为 Master 设备。

8.1.5 VRRP 的两种主备模式

在 VRRP 的主备应用中，根据不同的应用需求可以配置为主备备份和负载分担两种模式。下面分别予以介绍。

1. VRRP 主备备份模式

主备备份模式是 VRRP 提供备份功能的基本模式，就是同一时间仅由 Master 设备负责业务数据的处理，所有 Backup 设备均仅处于待命备份状态，不进行业务数据的处理，仅在当前 Master 设备出现故障时，再从 Backup 设备中选举一台设备成为新的 Master 设

备，接替原来 Master 设备的业务处理工作。

图 8-5 所示为一个 VRRP 主备备份模式的示例。在所建立的虚拟路由器中包括一个 Master 设备和两台 Backup 设备。

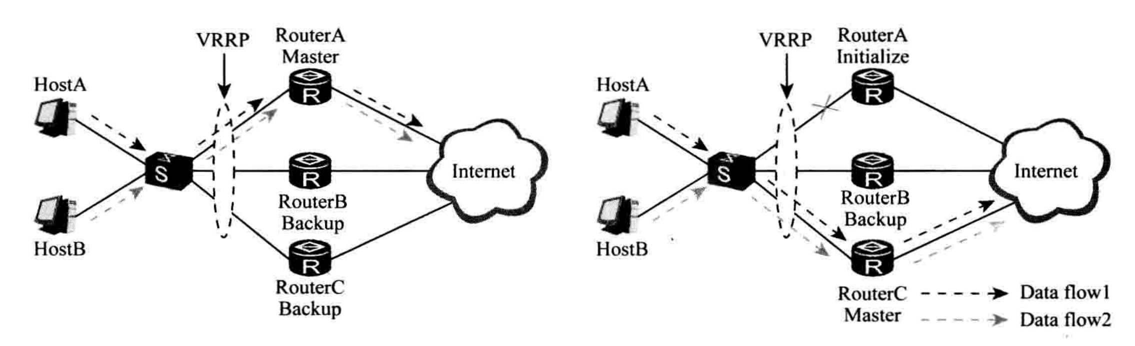


图 8-5　VRRP 主备备份模式示例

正常情况下，RouterA 为 Master 设备并承担业务转发任务，RouterB 和 RouterC 为 Backup 设备且不承担业务转发。RouterA 定期发送 VRRP 通告报文通知 RouterB 和 RouterC 自己工作正常。如果 RouterA 发生故障，RouterB 和 RouterC 会根据上节介绍的选举规则重新选举新的 Master 设备，继续为主机提供数据转发服务，实现网关备份的功能。

当 RouterA 故障恢复后，在抢占方式下，将重新抢占为 Master，因为它的优先级比 RouterB 和 RouterC 设备的高，除非它们中至少有一台修改为比 RouterA 更高的优先级；在非抢占方式下，RouterA 将继续保持为 Backup 状态，直到新 Master 设备出现故障时才有可能通过重新选举成为 Master 状态。

2. VRRP 负载分担模式

以上主备备份模式显然有些浪费资源了，因为大多数时间 Backup 设备都没有发挥作用，所以通常采用的是“VRRP 负载分担模式”。负载分担模式可以充分发挥每台 VRRP 设备的业务处理能力。但要注意的是，负载分担模式需要建立多个指派不同设备为 Master 设备的 VRRP 备份组，同一台 VRRP 设备可以加入多个备份组，在不同的备份组中具有不同的优先级。但每个备份组与 VRRP 主备备份模式的基本原理和报文协商过程都是相同的，对于每一个 VRRP 备份组，也都包含一个 Master 设备和若干 Backup 设备。

负载分担的实现方式有以下两种。

（1）多网关负载分担

通过创建多个带虚拟 IP 地址的 VRRP 备份组，为不同的用户指定不同的 VRRP 备份组作为网关，实现负载分担。这是最常用的负载分担方式。

在图 8-6 所示的网络中，配置了两个 VRRP 备份组：在 VRRP 备份组 1 中，RouterA 为 Master 设备，RouterB 为 Backup 设备；在 VRRP 备份组 2 中，RouterB 为 Master 设备，RouterA 为 Backup 设备。

这样就可以使一部分用户（如一个 VLAN 中的用户）将 VRRP 备份组 1 作为网关，另一部分用户（如另一个 VLAN 中的用户）将 VRRP 备份组 2 作为网关。这样既可实现对基于不同用户（如基于 VLAN）的业务流量的负载分担，同时又起到了相互备份的作用。

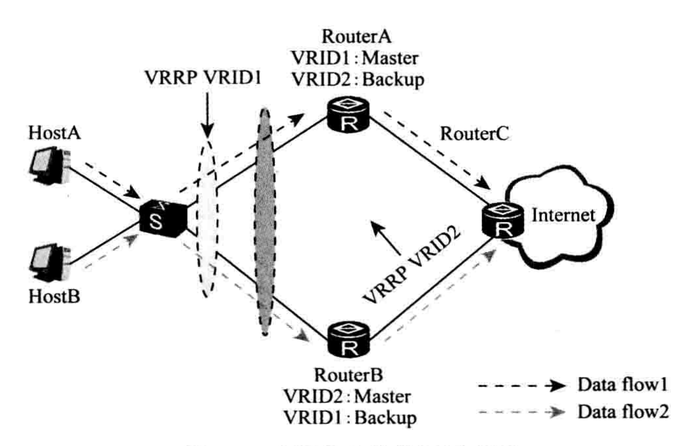


图 8-6 多网关负载分担示意图

（2）单网关负载分担

这种方式是通过创建带有虚拟路由器 IP 地址的 VRRP LBRG（Load-Balance Redundancy Group，负载分担管理组），并向该负载分担管理组中加入成员 VRRP 备份组（**无需配置虚拟路由器 IP 地址**），指定负载分担管理组 IP 地址作为所有用户的网关，来实现负载分担的。

单网关负载分担方式是前面介绍的多网关负载分担方式的升级版。通过创建 VRRP 负载分担备份组，可以在实现不同的用户共用同一个网关的同时实现负载分担，从而简化了用户侧的配置，便于维护和管理。本章不介绍这种负载分担方式。

下面仍以图 8-6 为例进行介绍。配置两个 VRRP 备份组：在 VRRP 备份组 1 中，RouterA 作为 Master 设备，RouterB 作为 Backup 设备；VRRP 备份组 2 中，RouterB 作为 Master 设备，RouterA 作为 Backup 设备。然后创建一个负载分担管理组，把 VRRP 备份组 1 和 VRRP 备份组 2 加入其中，并把 VRRP 备份组 1 作为管理组，VRRP 备份组 2 作为成员组。这样一来，所有用户都将负载分担管理组的 IP 地址作为网关。在收到用户侧的 ARP 请求报文时，VRRP 备份组 1 随机将自己的虚拟 MAC 地址或者 VRRP 备份组 2 的虚拟 MAC 地址封装到 ARP 响应报文，对 ARP 请求报文进行应答，进而实现负载分担。

8.1.6 VRRP 的两种延伸功能

在华为 AR G3 系列路由器（同时适用于 S 系列三层交换机）中，为了解决一些实际的问题，提供了两种延伸 VRRP 功能，即 VRRP 平滑倒换和管理 VRRP 备份组。下面分别予以介绍。

1. VRRP 平滑倒换

在一些较高端的 AR G3 系列路由器中往往安装有多块具有主、备性质的主控板，这时就涉及 VRRP 备份组在多块主控板间的倒换问题。因为在 Master 设备进行主控板的主、备倒换期间，Master 设备可能无法正常发送 VRRP 协议报文，所以 Backup 设备在 Master_Down_Interval 定时器超时后，会由于收不到 Master 设备发送的 VRRP 通告报文而自动切换为 Master。而当原 Master 设备完成主、备主控板的倒换后，由于原 Master

设备的优先级高于新 Master 设备，在抢占模式下会重新抢占成为 Master，从而引起链路两次切换，导致系统业务流量的不稳定。

为了避免主、备主控板倒换对业务流量的影响，可以在 Master 设备上使能 VRRP 平滑倒换功能。它的基本实现原理如下。

① Master 设备主控板的主、备倒换启动前，首先保存当前配置的 VRRP 通告报文发送间隔，然后调整 VRRP 通告报文发送间隔（一般远大于倒换前的发送间隔），并以新的时间间隔发送通告报文。同时，在平滑倒换前必须在 Backup 设备上使能 VRRP 报文时间间隔学习功能。

② 使能了 VRRP 报文时间间隔学习功能后，Backup 设备收到 Master 设备发送的 VRRP 通告报文时，会检查报文中的发送时间间隔值，如果和自己的不同，Backup 设备就会学习报文中的时间间隔，并调整自己的协议报文时间间隔值，使其与报文中的值保持一致。

③ 倒换结束后，Master 设备恢复倒换前的报文发送间隔设置，并以新的时间间隔发送通告报文。Backup 设备收到报文后会再一次学习时间间隔。

注意 VRRP 平滑倒换功能还依赖于 Master 设备系统本身。如果设备自身从主备倒换一开始系统便非常繁忙，无法调度 VRRP 模块运行的情况，VRRP 平滑倒换功能无效。

2. 管理 VRRP 备份组

为了提高网络可靠性，通常部署 NPE（Network Premise Equipment，网络前端设备）主备双属，也就是通过配置不同的 VRRP 备份组来指派同一设备属于不同的 VRRP 设备角色。但这样一来，每个 VRRP 备份组都需要维护自己的状态机，NPE 之间就会存在大量的 VRRP 报文。为了减少协议报文对带宽的占用及 CPU 资源的消耗，可以将其中一个 VRRP 备份组配置为管理 VRRP 备份组（mVRRP），其余的业务 VRRP 备份组与管理 VRRP 备份组进行绑定。

通过这种方式，可以实现管理 VRRP 负责发送协议报文来协商设备的主备状态；业务 VRRP 不发送协议报文，其主备状态与管理 VRRP 的主备状态保持一致，可以大大减少协议报文对 CPU 与带宽资源的消耗。图 8-7 所示为管理 VRRP 的应用示例。

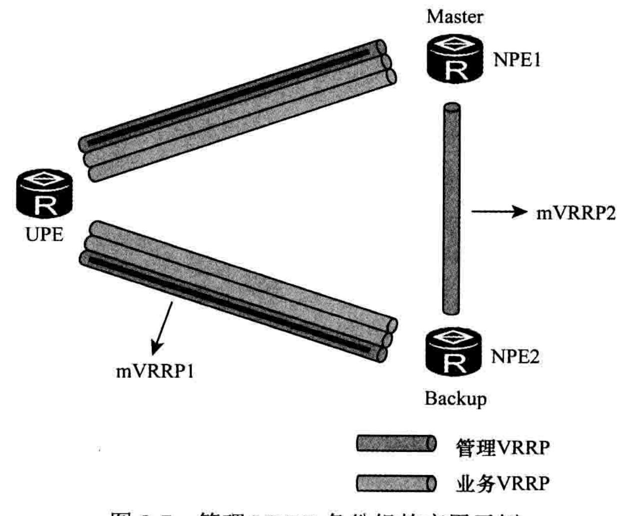


图 8-7 管理 VRRP 备份组的应用示例

管理 VRRP 备份组有两种角色。

① 当管理 VRRP 备份组作为网关使用时（如图中的 mVRRP1），管理 VRRP 既负责协商设备的主备状态，又承担业务流量。此时，在配置管理 VRRP 之前必须先创建普通 VRRP 备份组并配置虚拟 IP 地址，该虚拟 IP 地址即为用户设置的网关地址。

② 当管理 VRRP 备份组不作为网关使用时（如图中的 mVRRP2），管理 VRRP 只负责协商设备的主备状态，不承担业务流量。因此管理 VRRP 不需要具有虚拟 IP 地址，用户可以直接在接口上创建管理 VRRP 备份组。该配置在一定程度上降低了用户维护的复杂度。

8.1.7 支持的 VRRP 主要特性

在基于 IPv4 网络中的 VRRP 中，AR G3 系列路由器支持的 VRRP 特性包括以下所示的 VRRP 基本功能和 VRRP 联动功能。根据不同的应用需求，可以选择配置这两种功能。

① 配置 VRRP 基本功能：包括前面在 8.1.5 小节介绍的 VRRP 主备备份方式和 VRRP 负载分担方式。VRRP 主备备份是 VRRP 实现网关备份的基本方式；VRRP 负载分担通过配置多个 VRRP 备份组，在实现网关备份的同时，也实现流量的负载分担。

② 配置 VRRP 联动功能：通过与其他技术的联动，使得 VRRP 在自身或上行链路故障时能够及时感知并进行主备切换。配置 VRRP 基本功能后，可以配置 VRRP 联动功能，以优化 VRRP 主备切换功能，进一步增强网络的可靠性。

1. VRRP 主备备份

通过配置 VRRP 主备备份可以将多台设备虚拟成一台网关设备，其中包括一个 Master 设备和若干个 Backup 设备组。正常情况下，用户侧的流量通过 Master 设备转发。当 Master 设备出现故障时，通过 VRRP 协商，从 Backup 设备选举出新的 Master 设备，继续承担流量转发工作，实现了网关的冗余备份。具体参见 8.1.6 小节介绍。

2. VRRP 负载分担

VRRP 负载分担可以配置多个 VRRP 备份组，其中每个备份组都由一个 Master 设备和若干 Backup 设备组成，且 VRRP 备份组的 Master 设备各不相同。通过将每个备份组分别配置为部分主机的缺省网关，实现了流量转发的负载分担，同时，也实现了网关的相互备份。具体参见 8.1.6 小节介绍。

3. VRRP 联动功能

可以通过配置 VRRP 监控其他特性状态，使被监控的对象状态发生变化时通知 VRRP 进行主备切换，提高 VRRP 主备切换效率。AR G3 系列路由器支持联动对象及应用场景如表 8-3 所示。

表 8-3 VRRP 联动对象和应用场景

联动对象	应用场景
联动接口状态监视上行接口	当 Master 设备上行接口故障时，VRRP 是无法感知的，这也会导致业务中断。通过联动配置 VRRP 监视上行接口状态，当被监视的上行接口故障时及时调整 Master 设备优先级，触发 VRRP 主备切换，可减小上行接口故障对业务转发的影响

（续表）

联动对象	应用场景
联动 BFD 监视主备链路	当 VRRP 备份组故障时，Backup 设备需要等待 Master_Down_Interval 定时器超时后才能感知故障并进行切换，而且切换时间通常在 3 s 以上，在等待切换的这段时间内，仍会有发往 Master 设备的业务流，此时就会造成用户流量丢失。通过联动 BFD，使用 BFD 会话快速检测 VRRP 备份组间的通信故障，并及时通知 VRRP 备份组升高 Backup 设备的优先级，立即触发主备切换，实现了毫秒级的切换速度，可减少流量丢失。**有关 BFD 的详细介绍参见本书第 7 章**
联动 BFD 监视上行链路	当 VRRP 备份组**上行链路**出现故障时，VRRP 也是无法感知的，也会导致业务中断。通过联动 BFD（双向转发检测），使用 BFD 会话检测设备上行链路状态，当 BFD 检测到上行链路故障时及时通知 VRRP 备份组降低 Master 设备优先级，触发主备切换，减小链路故障对业务转发的影响 BFD 可以实现毫秒级的故障检测，联动 BFD 可以快速检测故障，从而使主备切换速度更快
联动 NQA 监视上行链路	也可以通过联动 NQA（网络质量分析）来解决在 VRRP 备份组**上行链路**出现故障时无法感知的不足。使用 NQA 测试例检测设备上行链路的状态，当 NQA 检测到上行链路故障时通知 VRRP 备份组调整优先级，触发主备切换，减小链路故障对业务转发的影响。**有关 NQA 的详细介绍，请参见本书第 7 章** NQA 可以对响应时间、网络抖动、丢包率等网络信息进行统计，通过配置 NQA 测试失败百分比，联动 NQA 还可以实现在上行链路质量较差时触发主备切换
联动路由监视上行链路	也可以通过联动路由来解决在 VRRP 备份组**上行链路**出现故障时无法感知的不足。使用 VRRP 监控设备上行转发路径路由条目，当上行转发路由条目撤销或是变为非活跃状态时通知 VRRP 备份组调整优先级，触发主备切换，减小链路故障对业务转发的影响 联动路由时的链路切换时间依赖于 VRRP 所联动路由协议的收敛速度

8.2 VRRP 基本功能配置与管理

VRRP 基本功能的配置很简单，最基本的配置就两个方面：一是创建 VRRP 备份组（如果要实现负载分担，则要创建多个以不同设备担当 Master 设备的 VRRP 备份组），二是配置用于 Master 设备选举的各 VRRP 备份组成员设备的优先级。另外，还可以配置一些可选功能（如抢占功能、VRRP 认证功能等）或时间参数（如 VRRP 通告报文发送时间间隔、VRRP 免费 ARP 报文超时定时器、VRRP 备份组抢占延时、VRRP 备份组状态恢复延时时间）。

总体来讲，VRRP 的基本功能包括以下主要配置任务（**只有前面两项为必选配置任务，且需要在 VRRP 备份组中每台路由器上配置**），但在配置 VRRP 基本功能前，要配置各设备 VRRP 接口的网络层属性，使其路由可达。

① 创建 VRRP 备份组。

② 配置设备在备份组中的优先级。

③（可选）配置 VRRP 的时间参数。

④（可选）配置 VRRP 报文在 super-vlan 中的发送方式。

⑤（可选）配置禁止检测 VRRP 报文跳数。

⑥（可选）配置 VRRP 报文的认证方式。

⑦（可选）配置 VRRP 版本：其实不需要配置，因为本书介绍的仅为 VRRPv2 版本，而缺省就为 v2 版本。

⑧（可选）使能虚拟地址可达性功能。

8.2.1 创建 VRRP 备份组

VRRP 备份组能够在不改变组网的情况下，采用将多台设备虚拟成一台网关设备，将虚拟交换机设备的 IP 地址作为用户的缺省网关的方式实现下一跳网关的备份。配置 VRRP 备份组后，流量通过 Master 设备转发，当 Master 设备故障时能迅速选举出新的 Master 设备继续承担流量转发任务，实现了网关冗余备份。如果在网关冗余备份的同时要实现对流量的负载分担，则可以配置不同的设备担当 Master 设备的多个 VRRP 备份组。

VRRP 备份组的创建方法很简单，就是在 VRRP 接口（**即 VRRP 设备的下行接口，可以是物理接口、逻辑接口或者子接口**）视图下通过 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* 命令创建。命令中的参数说明如下。

① *virtual-router-id*：指定所创建的 VRRP 备份组号，取值范围为 1～255 的整数。

② *virtual-address*：指定所创建的 VRRP 备份组的虚拟 IP 地址。**虚拟路由器的 IP 地址必须和对应接口的真实 IP 地址在同一网段**，如果配置了不在同网段的虚拟路由器的 IP 地址，该备份组会处于 VRRP 尚未配置的初始状态，此状态下，VRRP 不起作用。

对于网络中具有相同 VRRP 可靠性需求的用户，为了便于管理，并避免用户侧缺省网关地址随 VRRP 配置而改变，**可以为同一个备份组配置多个虚拟 IP 地址（也都必须与对应接口 IP 地址在同一网段），不同的虚拟 IP 地址为不同用户群服务**，每个备份组最多可配置 16 个虚拟 IP 地址。

说明 如果下游设备上送至网关的报文中带有 VLAN Tag，则需要进入子接口视图，并根据实际情况进行如下配置。

① 报文中带有一层 Tag 时，先要通过 **dot1q termination vid** *vid* 子接口视图命令配置对指定 Tag 的终结功能，然后在后面配置 **dot1q vrrp vid** *vid* 子接口视图命令配置用指定 Tag 值的 Dot1q 数据报文来维护 VRRP 状态。两命令中的参数 *vid* 用来指定终结的单层 VLAN ID。

② 报文中带有两层 Tag 时，先要通过 **qinq termination pe-vid** *pe-vid* **ce-vid** *ce-vid* 子接口视图命令配置子接口对指定的两层 Tag 报文的终结功能，然后通过 **qinq vrrp pe-vid** *pe-vid* **ce-vid** *ce-vid* 子接口视图命令配置用指定的双层 Tag 的 QinQ 数据报文来维护 VRRP。两命令中的参数 *pe-vid* 和 ce-vid 分别用来指定终结的外层和内层 VLAN ID。

③ 在子接口上配置 VRRP 时，建议同时使用 **arp broadcast enable** 命令使能终结子接口的 ARP 广播功能，以允许对应终结子接口能转发广播报文。

有关单层和双层 VLAN Tag 的封装配置参见配套图书**《华为交换机学习指南》**。

在设备上同时配置 VRRP 和静态 ARP 时，需要注意以下几点。

① 保证同一备份组的两端设备上配置相同的备份组 ID。

② 备份组 ID 是基于接口，而不是基于全局的，即**不同接口之间的备份组 ID 可以**

相同，但各备份组之间的虚拟 IP 地址不能相同。

③ 在配置虚拟 IP 地址时，一定不要配置与用户主机相同的 IP 地址。如果用户主机 IP 地址和备份组虚拟 IP 地址相同，则本网段报文都将被发送到用户主机，从而导致本网段的数据不能被正确转发。

④ 当在 Dot1q 终结子接口、在 QinQ 终结子接口或者在 VLANIF 接口下配置 VRRP 时，不能将与这些接口相关的静态 ARP 表项对应的映射 IP 地址作为 VRRP 的虚拟地址，否则会导致设备之间转发不通；同理，当在 Dot1q 终结子接口、在 QinQ 终结子接口或者在 VLANIF 接口下配置 VRRP 后，再配置静态 ARP 表项时，不能指定 VRRP 的虚拟地址作为该静态 ARP 表项中对应的映射 IP 地址，否则也可能导致设备之间转发不通。

缺省情况下，设备上无 VRRP 备份组，可用 **undo vrrp vrid** *virtual-router-id* [**virtual-ip** *virtual-address*]命令删除指定 VRRP 备份组的虚拟 IP 地址。如果备份组中的虚拟 IP 地址被全部删除，则系统会自动将此备份组删除。

说明　如要实现多网关负载分担，则需要重复执行上述 VRRP 备份组创建步骤，在接口上配置两个或多个 VRRP 备份组，各备份组之间以备份组号（*virtual-router-id*）区分。

【示例 1】在路由器 GE 1/0/0 接口上创建一个 VRRP 备份组，其中备份组号为 1，虚拟 IP 地址为 10.10.10.10。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.10.10.10
```

【示例 2】在路由器 GE 2/0/0.1 子接口上终结 VLAN 10，并创建一个 VRRP 备份组，其中备份组号为 1，虚拟 IP 地址为 100.1.1.111。

```
[Huawei] interface gigabitethernet 2/0/0.1
[Huawei -GigabitEthernet2/0/0.1] dot1q termination vid 10
[Huawei -GigabitEthernet2/0/0.1] arp broadcast enable
[Huawei -GigabitEthernet2/0/0.1] dot1q vrrp vid 10
[Huawei -GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 100.1.1.111
```

【示例 3】在路由器 GE 2/0/0.1 子接口上终结外层 VLAN 100，内层 VLAN 10，并创建一个 VRRP 备份组，其中备份组号为 1，虚拟 IP 地址为 100.1.1.111。

```
[Huawei] interface gigabitethernet 2/0/0.1
[Huawei -GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[Huawei -GigabitEthernet2/0/0.1] arp broadcast enable
[Huawei -GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[Huawei -GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 100.1.1.111
```

8.2.2 配置设备在备份组中的优先级

VRRP 根据优先级决定设备在备份组中的地位，优先级越高，越可能成为 Master 设备。通过配置优先级，可以指定 Master 设备，以承担流量转发业务。

VRRP 备份组中设备优先级是在对应的 VRRP 接口视图下使用 **vrrp vrid** *virtual-router-id* **priority** *priority-value* 命令进行配置的。命令中的参数说明如下。

① *virtual-router-id*：指定要配置当前路由器优先级的 VRRP 备份组号（在上节已创建）。

② *priority-value*：指定当前路由器在前面指定的 VRRP 备份组中的优先级，取值范

围为 1～254 的整数，数值越大，优先级越高。如果需要配置当前设备作为默认网关，可以执行此命令配置本设备在备份组中拥有最高的优先级，即指定其为 Master 设备。

注意 优先级 0 是系统保留作为特殊用途的，优先级值 255 保留给 IP 地址拥有者（即配置了路由器的某接口 IP 地址为虚拟路由器 IP 地址的路由设备）。**IP 地址拥有者的优先级不可配置，也不需要配置，直接为最高的 255。**

在 VRRP 备份组中设备优先级取值相同的情况下，先切换至 Master 状态的设备为 Master 设备，其余 Backup 设备不再进行抢占；如果同时竞争 Master，则比较 VRRP 备份组所在 VRRP 接口的 IP 地址大小，IP 地址较大的接口所在的设备当选为 Master 设备。

缺省情况下，优先级的取值是 100，可用 **undo vrrp vrid** *virtual-router-id* **priority** 命令恢复设备在指定 VRRP 备份组中的优先级为缺省值。

【示例】配置路由器在 VRRP 备份组 1 中的优先级为 150。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 priority 150
```

8.2.3 配置 VRRP 的时间参数

VRRP 所涉及的时间参数包括 VRRP 通告报文的发送间隔、路由器在 VRRP 备份组中的抢占延时、Master 设备发送免费 ARP 报文的超时时间和 VRRP 备份组的状态恢复延迟时间，具体说明如表 8-4 所示。它们都有对应的缺省值，且一般情况下无需修改，故本项配置任务可根据实际需要选择配置。

表 8-4 VRRP 时间参数

功能	说明
VRRP 通告报文的发送间隔	Master 设备会以 Advertisement_Interval 为定时器向组内的 Backup 设备发送 VRRP 通告报文，通告自己工作正常。如果 Backup 设备在 Master_Down_Interval 定时器超时后仍未收到 VRRP 通告报文，则重新选举 Master 网络流量过大或设备的定时器差异等因素可能会导致 Backup 设备无法及时接收到 VRRP 报文而发生状态转换，当原 Master 发送的报文到达新 Master 时，新 Master 将再次发送状态切换。这时，通过延长 Master 设备发送 VRRP 报文的时间间隔可以解决此类问题
路由器在 VRRP 备份组中的抢占延时	在不稳定的网络中，可能存在 VRRP 备份组监测的 BFD 等状态频繁振荡或 Backup 设备不能及时收到 VRRP 通告报文的情况，导致 VRRP 发生频繁切换而造成网络振荡。通过调整路由器在 VRRP 备份组中的抢占延时，可使 Backup 设备在指定的时间后再进行抢占，有效避免了 VRRP 备份组状态的频繁切换
Master 设备发送免费 ARP 报文的超时时间	在 VRRP 备份组中，为了确保下游交换机的 MAC 表项正确，Master 设备会定时发送免费 ARP 报文，用来刷新下游交换机上的 MAC 地址表项
VRRP 备份组的状态恢复延迟时间	在不稳定的网络中，VRRP 备份组监测的 BFD 或接口等状态频繁振荡会导致 VRRP 备份组状态频繁切换。通过配置 VRRP 备份组的状态恢复延迟时间，VRRP 备份组在接收到接口或 BFD 会话的 Up 事件时不会立刻响应，而是等待配置的状态恢复延迟时间后，再进行相应的处理，防止因接口或 BFD 会话的频繁振荡而导致的 VRRP 状态的频繁切换

以上 VRRP 时间参数的具体配置步骤如表 8-5 所示。

表 8-5　**VRRP 时间参数的配置步骤**

步骤	命令	说明
1	**system-view** 例如：<Huawei>**system- view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 VRRP 接口，可以是物理接口、逻辑接口或者子接口，进入接口视图
3	**vrrp vrid** *virtual-router-id* **timer advertise** *advertise-interval* 例如：[Huawei-GigabitEthernet1/0/0]**vrrp vrid 1 timer advertise** 5	配置路由器发送 VRRP 通告报文的时间间隔。命令中的参数说明如下 • *virtual-router-id*：指定要配置 VRRP 通告报文发送时间间隔的 VRRP 备份组的 ID • *advertise-interval*：指定备份组中的 Master 设备发送 VRRP 通告报文的时间间隔，如果是 v2 版本，则取值范围为 1～255 的整数，如果是 v3 版本，则取值范围为 1～40 的整数，单位是 s 缺省情况下，发送 VRRP 通告报文的时间间隔是 1 s，可用 **undo vrrp vrid** *virtual-router-id* **timer advertise** 命令恢复指定 VRRP 备份组中 Master 发送 VRRP 报文的时间间隔为缺省值
4	**vrrp vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value* 例如：[Huawei-GigabitEthernet1/0/0] **vrrp vrid 1 preempt-mode timer delay** 5	配置路由器为延迟抢占方式，并配置抢占延迟时间。命令中的参数说明如下 • *virtual-router-id*：指定要配置路由器抢占延迟时间的 VRRP 备份组的 ID • *delay-value*：指定路由的抢占延迟时间，取值范围为（0～3 600）的整数秒 缺省情况下，抢占延迟时间为 0，即为立即抢占。立即抢占方式下，Backup 设备一旦发现自己的优先级比当前的 Master 的优先级高，就会抢占成为 Master，用执行 **undo vrrp vrid** *virtual-router-id* **preempt-mode** 命令可以恢复缺省的立即抢占方式 【说明】可以执行 **vrrp vrid** *virtual-router-id* **preempt-mode disable** 命令设置对应 VRRP 备份组中的路由器采用非抢占方式。在非抢占方式下，一旦备份组中的某台路由器成为 Master，只要它没有出现故障，其他路由器即使随后被配置更高的优先级也不会成为 Master。在配置 VRRP 备份组内各路由器的延迟方式时建议 Backup 设备配置为立即抢占，Master 设备配置为延时抢占，指定一定的延迟时间。这样配置的目的是为了在网络环境不稳定时，为上下行链路的状态恢复一致性等待一定时间，以免出现双 Master 设备或由于主备双方频繁抢占导致用户设备学习到错误的 Master 设备地址 抢占延迟时间需根据网络情况合理配置，对于较稳定的网络，可以配置较小的抢占延迟时间，避免 Master 故障后，Backup 设备长时间没有切换成 Master 而导致的流量丢失；对于不稳定的网络，可以配置较大的抢占延迟时间，避免由于 VRRP 状态频繁切换而导致流量丢失
5	**quit** 例如：[Huawei-GigabitEthernet1/0/0] **quit**	退出接口视图，返回系统视图

（续表）

步骤	命令	说明
6	**vrrp recover-delay** *delay-value* 例如：[Huawei] **vrrp recover-delay** 5	配置当前路由器在 VRRP 备份组的状态恢复延迟时间，取值范围为 0～60 的整数秒。执行此命令后，该路由器上所有 VRRP 备份组配置了相同的状态恢复延迟时间 缺省情况下，VRRP 备份组状态恢复延迟时间为 0 s，可用 **undo vrrp recover-delay** 命令恢复 VRRP 备份组的状态恢复延迟时间为缺省值
7	**vrrp gratuitous-arp timeout** *time* 例如：[Huawei] **vrrp gratuitous-arp timeout** 100	配置当前路由器 Master 发送免费 ARP 报文的超时时间，取值范围为（30～1 200）的整数秒。配置的 Master 设备发送免费 ARP 报文超时时间应小于用户侧设备的 MAC 地址表项老化时间，否则太快地发送免费报文就没什么意义了 缺省情况下，Master 每隔 120 s 发送一次免费 ARP 报文，可用 **undo vrrp gratuitous-arp timeout** 命令恢复 Master 发送免费 ARP 报文的超时时间为缺省值。如果不需要发送免费 ARP 报文，则在系统视图下执行 **vrrp gratuitous-arp timeout disable** 命令

8.2.4 配置其他可选功能

最后将介绍其他几项可选功能的配置，具体如下。

（1）VRRP 版本

可配置 VRRPv2 和 VRRPv3 版本，缺省为 VRRPv2 版本，而本章仅介绍 VRRPv2 版本，故实际上可不用配置。

（2）（可选）使能虚拟地址可达性功能

路由器支持对虚拟 IP 地址的 Ping 功能，可用于检测备份组中的 Master 设备是否有效，以确认是否能通过使用某虚拟 IP 地址作为默认网关与外部通信。

（3）（可选）配置禁止检测 VRRP 报文跳数

系统对收到的 VRRP 通告报文的 TTL 值进行检测，如果 TTL 值不等于 255，则丢弃这个报文。在不同设备制造商的设备配合使用的组网环境中，检测 VRRP 报文的 TTL 值可能导致错误地丢弃合法报文，此时用户可以配置系统不检测 VRRP 报文的 TTL 值，以实现不同设备制造商设备之间的互通。

（4）（可选）配置 VRRP 报文的认证方式

在一些不安全的网络环境中，需要配置 VRRP 报文认证，以确保路由器对要发送和接收的 VRRP 报文都是真实、合法的。VRRP 提供了简单字符（Simple）认证方式或 MD5 认证方式。

① 简单字符（Simple）认证：发送 VRRP 通告报文的路由器将认证方式和认证字填充到通告报文中，而收到通告报文的路由器则会将报文中的认证方式和认证字符与本端配置的认证方式和认证字符进行匹配。如果相同，则认为接收到的报文是合法的 VRRP 通告报文；否则认为接收到的报文是一个非法报文，并丢弃这个报文。

② MD5 认证：发送 VRRP 通告报文的路由器利用 MD5 算法对认证字符进行加密，加密后保存在 Authentication Data 字段中。收到通告报文的路由器会对报文中的认证方式和解密后的认证字符进行匹配，检查该报文的合法性。它比简单字符认证更

安全。

（5）（可选）配置 VRRP 报文在 super-vlan 中的发送方式

当 VRRP 备份组配置在聚合 VLAN 时，用户可以通过命令行配置，使 VRRP 报文在指定的 sub-VLAN 中传输，避免 VRRP 通告报文在所有 sub-VLAN 内广播，以节约网络带宽。

以上 5 项配置任务的具体配置步骤如表 8-6 所示。

表 8-6　VRRP 其他功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**vrrp version** { v2 | v3 } 例如：[Huawei] **vrrp version v2**	配置当前设备的 VRRP 协议版本号。v2 版本的 VRRP 备份组，只能发送和接收 v2 版本的 VRRP 通告报文，如果接收到 v3 版本的 VRRP 通告报文，则该备份组将此报文丢弃；v3 版本的 VRRP 备份组，可以接收 v2 和 v3 版本的 VRRP 通告报文，通过配置发送报文的版本模式可以实现与 v2 及 v3 版本设备间的通信 缺省情况下，VRRP 协议版本号为 2，可用 **undo vrrp version** 命令恢复当前设备的 VRRP 协议版本号为缺省值
3	**vrrp virtual-ip ping enable** 例如：[Huawei]**vrrp virtual-ip ping enable**	使能 Master 设备响应 Ping 报文 缺省情况下，Master 设备响应 Ping 报文处于使能状态，可用 **undo vrrp virtual-ip ping enable** 命令去使能 Master 设备响应 Ping 报文。使能虚拟 IP 地址可达性开关后，外部网络能够 Ping 通虚拟 IP 地址，带来可能遭受 ICMP 攻击的隐患，可以执行 **undo vrrp virtual-ip ping enable** 命令关闭虚拟地址可达性开关
4	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 VRRP 接口，可以是物理接口、逻辑接口或者子接口，进入接口视图
5	**vrrp un-check ttl** 例如：[Huawei-GigabitEthernet1/0/0]**vrrp un-check ttl**	禁止检测 VRRP 报文的 TTL 值。按照 RFC 2338 的规定，系统对收到的 VRRP 报文的 TTL 值进行检测，如果 TTL 值不等于 255，则丢弃这个报文，并打印出 VRRP 报文错误的日志信息 在某些组网环境中，尤其是与不同厂商的设备配合使用时，这种处理方式可能导致错误地丢弃报文。这时可以配置系统不检测 VRRP 报文的 TTL 值 缺省情况下，系统检测 VRRP 报文的 TTL 值，可用 **undo vrrp un-check ttl** 命令恢复对 VRRP 报文 TTL 值的检测情况为缺省值
6	**vrrp vrid** *virtual-router-id* **authentication-mode** { **simple** { *key* | **plain** *key* | **cipher** *cipher-key* } | **md5** *md5-key* } 例如：[Huawei-GigabitEthernet1/0/0]**vrrp vrid 1 authentication-mode simple** huawei	配置 VRRP 备份组的认证方式和认证字符。命令中的参数和选项说明如下 • *virtual-router-id*：指定要配置 VRRP 认证方式的 VRRP 备份组号 • **simple**：二选一选项，指定采用 Simple 认证方式 • *key*：多选一参数，指定 Simple 认证方式的认证字符，1～8 个字符，不支持空格，**区分大小写** • **plain** *key*：多选一参数，指定明文认证方式的认证字符，1～8 个字符，不支持空格，**区分大小写**

（续表）

步骤	命令	说明
6	**vrrp vrid** *virtual-router-id* **authentication-mode** { **simple** { *key* | **plain** *key* | **cipher** *cipher-key* } | **md5** *md5-key* } 例如：[Huawei-GigabitEthernet1/0/0]**vrrp vrid 1 authentication-mode simple** huawei	● **cipher** *cipher-key*：多选一参数，指定密文认证方式的认证字符，可以是明文字符，也可以是密文字符，明文长度为1～8个字符，密文长度为32个字符，不支持空格，**区分大小写** ● **md5** *md5-key*：二选一参数，指定MD5认证方式的认证字符，也可以是明文字符，或者密文字符，明文长度为1～8个字符，密文长度为24个或者32个字符，不支持空格，**区分大小写**。因为符号^#^#和$@$@用来识别变长密码，^#^#作为新密码的前缀和后缀，$@$@作为老密码的前缀和后缀，所以不支持以"$@$@"或"^#^#"同时作为明文密码的起始和结束字符 同一VRRP备份组的认证方式和认证字符必须相同，否则Master设备和Backup设备无法协商成功 缺省情况下，VRRP备份组采用无认证方式，可用 **undo vrrp vrid** *virtual-router-id* **authentication-mode** 命令取消指定VRRP备份组的认证方式和认证
7	**quit** 例如：[Huawei-GigabitEthernet1/0/0]	退出接口视图，返回系统视图
8	**interface** *interface-type interface-number* 例如：[Huawei] **interface vlanif 100**	键入在Super-Vlan中要发送VRRP通告报文Super-VLAN中的VLANIF接口，进入接口视图 **仅当是在VLANIF接口下配置VRRP备份组时才需要配置**
9	**vrrp advertise send-mode** { *sub-vlan-id* | **all** } 例如：[Huawei-Vlanif100] **vrrp advertise send-mode** 5	配置在Super-Vlan中的VRRP通告报文发送方式，仅在相关Super-VLAN中VLANIF接口上已经成功配置了VRRP备份组时才需要配置本任务。命令中的参数和选项说明如下 ● *sub-vlan-id*：二选一参数，指定Master设备要发送VRRP通告报文的sub-VLAN的VLAN ID ● **all**：二选一选项，指定Master设备向本super-VLAN的所有sub-VLAN发送VRRP通告报文，但这将对带宽的使用率造成影响 缺省情况下，Master设备向super-VLAN中状态为Up且VLAN ID最小的sub-VLAN发送VRRP通告报文，可用 **undo vrrp advertise send-mode** 命令恢复Master设备向super-VLAN中发送VRRP通告报文的方式为缺省值

8.2.5 VRRP基本功能管理

配置好VRRP基本功能后，可通过以下 **display** 任意视图命令查看配置信息，验证配置结果；或者查看VRRP报文统计信息，了解VRRP运行情况；也可以通过以下 **reset** 用户视图命令清除VRRP统计信息，以便了解最新的VRRP运行情况。

① **display vrrp** [**interface** *interface-type interface-number*] [*virtual-router-id*] [**brief**]，或 **display vrrp** [**admin-vrrp** | [**interface** *interface-type interface-number* [*virtual-router-id*] | *virtual-router-id*] [**verbose**]]：查看指定接口、指定VRRP备份组或者所有VRRP备份组的状态信息和配置参数。

② **display vrrp protocol-information**：查看VRRP的相关信息。

③ 执行 **display vrrp** [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics**：查看指定接口、指定 VRRP 备份组或者所有 VRRP 备份组的报文收发统计信息。

④ **reset vrrp** [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**：清除指定接口、指定 VRRP 备份组或者所有 VRRP 备份组的 VRRP 报文统计信息。

8.2.6 VRRP 主备备份配置示例

本示例的基本拓扑结构如图 8-8 所示，HostA 通过 Switch 双线连接到 RouterA 和 RouterB。用户希望实现：正常情况下，主机以 RouterA 为默认网关接入 Internet；而当 RouterA 故障时，RouterB 接替作为网关继续进行工作，实现网关的冗余备份；RouterA 故障恢复后，可以在 20 s 内重新成为网关（即抢占延时为 20 s）。

1. 基本配置思路分析

本示例仅要求实现主备备份，根据 8.2.1 小节和 8.2.2 小节介绍的配置方法（不需要配置其他可选配置任务）可以得出本示例基本配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使各设备间网络层连通。

② 在 RouterA 和 RouterB 上配置 VRRP 备份组。其中，RouterA 上配置较高优先级和 20 s 抢占延时，作为 Master 设备承担流量转发；RouterB 上配置较低优先级，作为备用路由器，实现网关冗余备份。

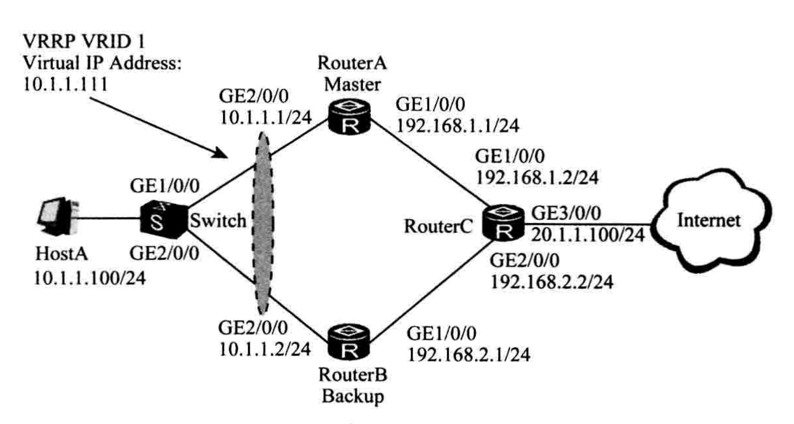


图 8-8　VRRP 主备备份配置示例拓扑结构

2. 具体配置步骤

（1）配置设备间的网络互连

首先配置设备各接口的 IP 地址，以 RouterA 为例。RouterB 和 RouterC 的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

然后配置 RouterA、RouterB 和 RouterC 间采用 OSPF 协议进行互连。以 RouterA 为

例，RouterB 和 RouterC 的配置与之类似，略。有关 OSPF 路由的配置将在本书后面介绍。

```
[RouterA] ospf 1                                          !---创建 OSPF 进程 1
[RouterA-ospf-1] area 0                                   !---创建骨干区域 0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255     !---宣告所直接连接的 10.1.1.0/24 网段
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255 !---宣告所直接连接的 192.168.1.0/24 网段
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

（2）配置 VRRP 备份组

在 RouterA 上创建 VRRP 备份组 1，配置虚拟路由器 IP 地址（**必须与对应的 VRRP 接口 IP 地址在同一网段**），并设置 RouterA 在该备份组中的优先级为 120、抢占时间为 20 s。

```
[RouterA] interface gigabitethernet 2/0/0                    !---进入到 VRRP 接口 GE2/0/0（下行接口）视图
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111    !---创建 1 号备份组，并配置 IP 地址为 10.1.1.111，一定要与 GE2/0/0 接口 IP 地址在同一网段
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120        !---配置 RouterA 在备份组 1 中的优先级为 120
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 preempt-mode timer delay 20 !---配置 RouterA 在备份组 1 中为抢占延时方式，延时时间为 20 s
[RouterA-GigabitEthernet2/0/0] quit
```

在 RouterB 上创建 VRRP 备份组 1，配置与 RouterA 上备份组 1 相同的虚拟 IP 地址，并配置其在该备份组中的优先级为缺省值 100，使它成为 Backup 设备。

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterB-GigabitEthernet2/0/0] quit
```

配置好后，可在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，查看 RouterA 在备份组中的状态为 Master，RouterB 在备份组中的状态为 Backup。输出示例如下。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State          : Master
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.1
    PriorityRun      : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 20 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-11 11:39:18
    Last change time : 2012-05-26 11:38:58
<RouterB> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State          : Backup
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.1
    PriorityRun      : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
```

```
        TimerRun : 1 s
        TimerConfig : 1 s
        Auth type : NONE
        Virtual MAC : 0000-5e00-0101
        Check TTL : YES
        Config type : normal-vrrp
        Create time : 2012-05-11 11:39:18
        Last change time : 2012-05-26 11:38:58
```

在 RouterA 的接口 GE2/0/0 上执行 **shutdown** 命令，模拟 RouterA 出现故障。再在 RouterB 上执行 **display vrrp** 命令查看 VRRP 状态信息，可看到 RouterB 的状态已是 Master，表明切换成功。输出示例如下。

```
<RouterB> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.2
    PriorityRun      : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-11 11:39:18
    Last change time : 2012-05-26 11:38:58
```

再在 RouterA 的接口 GE2/0/0 上执行 **undo shutdown** 命令，等待 20 s 后在 RouterA 上执行 **display vrrp** 命令查看 VRRP 状态信息，可看到 RouterA 的状态又恢复成 Master。输出示例如下。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] quit
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.1
    PriorityRun      : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 20 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-11 11:39:18
    Last change time : 2012-05-26 11:38:58
```

通过以上验证，表示配置是正确的。

8.2.7 VRRP 多网关负载分担配置示例

本示例的基本拓扑结构如图 8-9 所示，HostA 和 HostC 通过 Switch 双线连接到 RouterA 和 RouterB。用户希望 HostA 以 RouterA 为默认网关接入 Internet，RouterB 作为备份网关；HostC 以 RouterB 为默认网关接入 Internet，RouterA 作为备份网关，以实现流量的负载均衡。原 Master 设备故障恢复后，可以在 20 s 内重新成为网关。

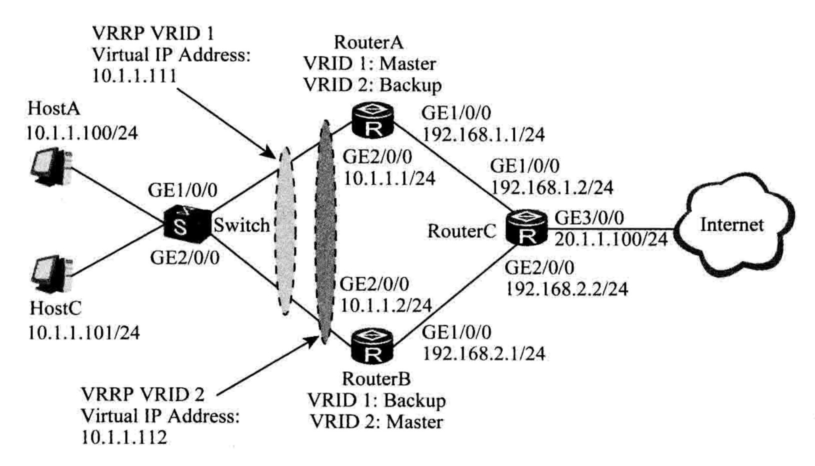


图 8-9 VRRP 多网关负载分担配置示例拓扑结构

1. 基本配置思路分析

本示例要求两台用户主机采用不同的设备作为默认网关实现流量的负载均衡，所以需要采用 VRRP 多网关负载分担方式，基本的配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使各设备间网络层连通。

② 在 RouterA 和 RouterB 上分别创建 VRRP 备份组 1 和 VRRP 备份组 2。在备份组 1 中，配置 RouterA 为 Master 设备，RouterB 为 Backup 设备；在备份组 2 中，配置 RouterB 为 Master 设备，RouterA 为 Backup 设备，以实现流量的负载均衡。

2. 具体配置步骤

（1）配置设备间的网络互连

首先配置设备各接口的 IP 地址，以 RouterA 为例。RouterB 和 RouterC 的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

然后配置 RouterA、RouterB 和 RouterC 间采用 OSPF 协议进行互连。以 RouterA 为例，RouterB 和 RouterC 的配置与之类似，略。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
```

```
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

（2）配置 VRRP 备份组

在 RouterA 和 RouterB 上分别创建 VRRP 备份组 1，并配置虚拟路由器 IP 地址（**必须与对应的 VRRP 接口 IP 地址在同一网段**），配置 RouterA 的优先级为 120、抢占延时为 20 s；RouterB 的优先级为缺省值 100（**这样可使在 VRRP 备份组 1 中 RouterA 的优先级更高**），使 RouterA 为 Master 设备，RouterB 为 Backup 设备。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111          !---要写 GE2/0/0 接口 IP 地址在同一网段
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 preempt-mode timer delay 20 !---配置抢占延时为 20 s
[RouterA-GigabitEthernet2/0/0] quit

[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterB-GigabitEthernet2/0/0] quit
```

在 RouterA 和 RouterB 上分别创建 VRRP 备份组 2，并配置虚拟路由器 IP 地址（**要与备份组 1 的虚拟 IP 地址不同，但也必须与对应的 VRRP 接口 IP 地址在同一网段**），这里要配置 RouterB 的优先级为 120，抢占延时为 20 s；RouterA 的优先级为缺省值 100（**这样可使在 VRRP 备份组 2 中 RouterB 的优先级更高**），使 RouterB 为 Master 设备，RouterA 为 Backup 设备。

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 10.1.1.112
[RouterB-GigabitEthernet2/0/0] vrrp vrid 2 priority 120
[RouterB-GigabitEthernet2/0/0] vrrp vrid 2 preempt-mode timer delay 20
[RouterB-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 10.1.1.112
[RouterA-GigabitEthernet2/0/0] quit
```

配置好后，可在 RouterA 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。输出示例如下。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State          : Master
    Virtual IP     : 10.1.1.111
    Master IP      : 10.1.1.1
    PriorityRun    : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES    Delay Time : 20 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-11 11:39:18
    Last change time : 2012-05-26 11:38:58
```

```
GigabitEthernet2/0/0 | Virtual Router 2
  State          : Backup
  Virtual IP     : 10.1.1.112
  Master IP      : 10.1.1.2
  PriorityRun    : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES    Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0102
  Check TTL : YES
  Config type : normal-vrrp
  Create time : 2012-05-11 11:40:18
  Last change time : 2012-05-26 11:48:58
```

同样，在 RouterB 上执行 **display vrrp** 命令，可以看到 RouterB 在备份组 1 中作为 Backup 设备，在备份组 2 中作为 Master 设备。输出示例略。

最后在 Switch 连接的用户主机上配置指向 VRRP 虚拟 IP 地址的网关即可。

8.2.8 Dot1q 终结子接口支持 VRRP 配置示例

本示例的基本拓扑结构如图 8-10 所示，局域网内的主机通过 Switch 双线连接到 RouterA 和 RouterB，Switch 上送的用户报文中带有一层 Tag。用户希望实现：正常情况下，主机以 RouterA 为默认网关接入 Internet，当 RouterA 故障时，RouterB 接替作为网关继续进行工作，实现网关的冗余备份；RouterA 故障恢复后，可以在 20 s 内重新成为网关。

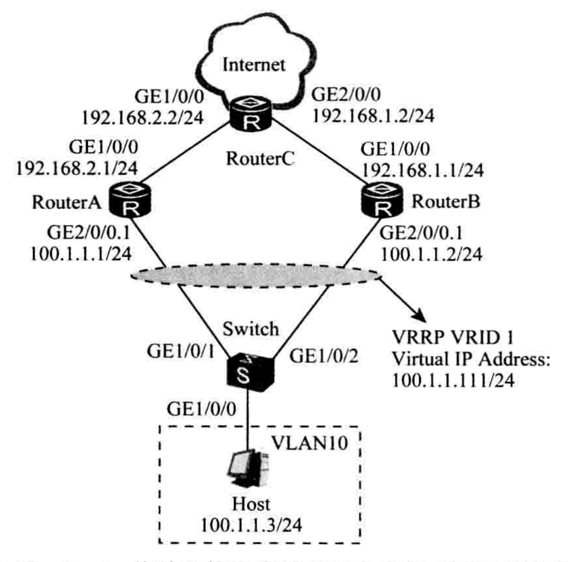


图 8-10 Dot1q 终结子接口支持 VRRP 配置示例的拓扑结构

1. 基本配置思路分析

本示例要封装一层 VLAN 标签，所以必须在路由器上配置子接口进行 Dot1q 终结，然后采用 Dot1q 终结子接口支持 VRRP 实现网关的冗余备份。其基本配置思路如下。

① 配置各设备接口IP地址及路由协议，使网络层路由可达。

② 在RouterA和RouterB的子接口上配置VRRP备份组，其中，RouterA上配置较高优先级和20 s抢占延时，作为Master设备承担流量转发；RouterB上配置较低优先级，作为备用路由器。

2. 具体配置步骤

（1）配置设备间的网络互连

先配置各路由器接口IP地址，现仅以RouterA为例，其余路由器的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] ip address 100.1.1.1 24
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.2.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

配置Switch的二层接口加入VLAN。

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface gigabitethernet 1/0/0
[Switch-GigabitEthernet1/0/0] port link-type access
[Switch-GigabitEthernet1/0/0] port default vlan 10
[Switch-GigabitEthernet1/0/0] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/2] quit
```

配置RouterA、RouterB和RouterC间采用OSPF协议进行互连。以RouterA为例，RouterB和RouterC的配置与之类似，略。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

（2）配置Dot1q终结子接口，并支持VRRP

在RouterA的子接口GE2/0/0.1上终结VLAN 10，创建VRRP备份组1，配置RouterA在该备份组中的优先级为120，并配置抢占时间为20 s。在RouterB的子接口GE2/0/0.1上终结VLAN 10，创建VRRP备份组1，其在该备份组中的优先级为缺省值100。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] dot1q termination vid 10 !---在GE2/0/0.1 子接口上终结 VLAN 10
[RouterA-GigabitEthernet2/0/0.1] arp broadcast enable !---使能终结子接口的ARP广播功能
[RouterA-GigabitEthernet2/0/0.1] dot1q vrrp vid 10          !—配置子接口使用VLAN 10报文维护VRRP状态，即支持VRRP协议
```

```
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 100.1.1.111        !---要与 GE2/0/0.1 子接口 IP 地址在同一网段
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] dot1q termination vid 10
[RouterB-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterB-GigabitEthernet2/0/0.1] dot1q vrrp vid 10
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 100.1.1.111
[RouterB-GigabitEthernet2/0/0.1] quit
```

完成上述配置后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组中的状态是 Master，RouterB 在备份组中的状态为 Backup。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0.1 | Virtual Router 1
    State            : Master
    Virtual IP       : 100.1.1.111
    Master IP        : 100.1.1.1
    PriorityRun      : 120
    PriorityConfig   : 120
    MasterPriority   : 120
    Preempt          : YES     Delay Time : 20 s
    TimerRun         : 1 s
    TimerConfig      : 1 s
    Auth Type        : NONE
    Virtual Mac      :  0000-5e00-0101
    Check TTL        : YES
    Config type      : normal-vrrp
    Create time : 2012-05-30 21:25:47
    Last change time : 2012-05-30 21:25:51
```

分别在 RouterA 和 RouterB 上执行 **display ip routing-table** 命令，RouterA 上可以看到路由表中有一条目的地址为虚拟 IP 地址的直连路由，而 RouterB 上该路由为 OSPF 路由，因为此时 RouterA 是担当 Master 设备，而 RouterB 为 Backup 设备。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      100.1.1.0/24  Direct 0    0           D   100.1.1.1       GigabitEthernet2/0/0.1
      100.1.1.1/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
      100.1.1.2/32  Direct 0    0           D   100.1.1.2       GigabitEthernet2/0/0.1
  100.1.1.111/32  Direct0     0           D   127.0.0.1       GigabitEthernet2/0/0.1
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   2           D   192.168.2.2     GigabitEthernet1/0/0
    192.168.2.0/30  OSPF    10   2           D   192.168.2.2     GigabitEthernet1/0/0
    192.168.2.1/32  Direct 0    0           D   127.0.0.1       GigabitEthernet1/0/0
    192.168.2.2/32  Direct 0    0           D   192.168.2.2     GigabitEthernet1/0/0

[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
```

```
Routing Tables: Public
        Destinations : 10          Routes : 10
Destination/Mask    Proto   Pre   Cost        Flags NextHop          Interface
      100.1.1.0/24  Direct 0      0             D   100.1.1.2        GigabitEthernet2/0/0.1
      100.1.1.1/32  Direct 0      0             D   100.1.1.1        GigabitEthernet2/0/0.1
      100.1.1.2/32  Direct 0      0             D   127.0.0.1        GigabitEthernet2/0/0.1
  100.1.1.111/32  OSPF   10    2             D   100.1.1.1        GigabitEthernet2/0/0.1
      127.0.0.0/8   Direct 0      0             D   127.0.0.1        InLoopBack0
      127.0.0.1/32  Direct 0      0             D   127.0.0.1        InLoopBack0
    192.168.1.0/24  Direct 0      0             D   192.168.1.1      GigabitEthernet1/0/0
    192.168.1.1/32  Direct 0      0             D   127.0.0.1        GigabitEthernet1/0/0
    192.168.1.2/32  Direct 0      0             D   192.168.1.2      GigabitEthernet1/0/0
    192.168.2.0/30  OSPF    10     2             D   192.168.1.2      GigabitEthernet1/0/0
```

在 RouterA 的接口 GE2/0/0.1 上执行 **shutdown** 命令，模拟链路故障。然后分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组中的状态切换为 Initialize，RouterB 在备份组中的状态切换为 Master。输出示例略。

然后在 RouterA 的接口 GE2/0/0.1 上执行 **undo shutdown** 命令，恢复链路故障。20 s 后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组中的状态恢复为 Master，RouterB 在备份组中的状态恢复为 Backup。输出示例略。

8.2.9　QinQ 终结子接口支持 VRRP 配置示例

本示例的基本拓扑结构如图 8-11 所示，局域网内的主机通过 SwitchA 双归属到 RouterA 和 RouterB，其中 HostA 属于 VLAN10，HostB 属于 VLAN20。SwitchA 上送的用户报文中带有两层 Tag。用户希望实现：正常情况下，主机以 RouterA 为默认网关接入 Internet，当 RouterA 故障时，RouterB 接替作为网关继续进行工作，实现网关的冗余备份；RouterA 故障恢复后，可以在 20 s 内重新成为网关。

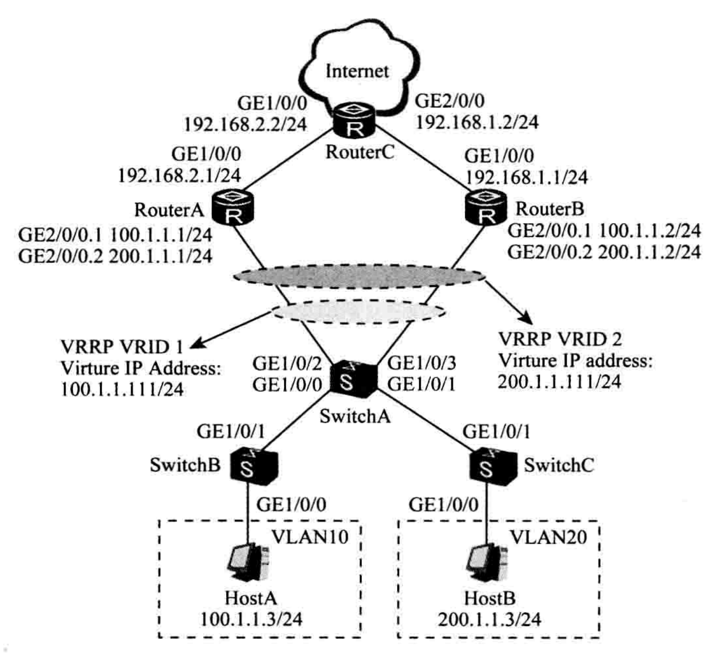


图 8-11　QinQ 终结子接口支持 VRRP 配置示例的拓扑结构

1. 基本配置思路分析

因为本示例中用户端主机分属于不同的 VLAN，所以需要采用 QinQ（双层 VLAN）封装方式的终结子接口，并使其支持 VRRP 实现网关的冗余备份。其基本配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

② 在 SwitchA 配置 QinQ，假设为 SwitchB 的 VLAN 数据封装外层 VLAN100，为 SwitchC 的 VLAN 数据封装外层 VLAN200。

③ 在 RouterA 和 RouterB 的子接口上配置 VRRP 备份组，其中，RouterA 上配置较高优先级和 20 s 抢占延时，作为 Master 设备承担流量转发；RouterB 上配置较低优先级，作为备用路由器。

2. 具体配置步骤

（1）配置各路由器接口的 IP 地址

配置各路由器接口（包括子接口，**但如果创建了子接口，则对应物理接口上不要配置 IP 地址**）的 IP 地址。仅以 RouterA 为例，其他路由器的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] ip address 100.1.1.1 24
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterA] interface gigabitethernet 2/0/0.2
[RouterA-GigabitEthernet2/0/0.2] ip address 200.1.1.1 24
[RouterA-GigabitEthernet2/0/0.2] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.2.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterA、RouterB 和 RouterC 间采用 OSPF 协议进行互连。仅以 RouterA 为例，RouterB 和 RouterC 的配置与之类似，略。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置各 Switch 的接口加入对应 VLAN 中，有关 VLAN 和 QinQ 方面的配置请参见《华为交换机学习指南》一书。

SwitchB 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname SwitchB
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface gigabitethernet 1/0/0
[SwitchB-GigabitEthernet1/0/0] port link-type access   !---指定 GE1/0/0 接口为 ACCESS 类型
[SwitchB-GigabitEthernet1/0/0] port default vlan 10   !---将 GE1/0/0 接口加入到 VLAN 10 中
[SwitchB-GigabitEthernet1/0/0] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk   !---指定 GE1/0/0 接口为 Trunk 类型
[SwitchB-GigabitEthernet1/0/1] port trunk allow-pass vlan 10 !---允许 GE1/0/0 接口通过 VLAN 10 数据
[SwitchB-GigabitEthernet1/0/1] quit
```

SwitchC 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname SwitchC
[SwitchC] vlan 20
[SwitchC-vlan10] quit
[SwitchC] interface gigabitethernet 1/0/0
[SwitchC-GigabitEthernet1/0/0] port link-type access
[SwitchC-GigabitEthernet1/0/0] port default vlan 20
[SwitchC-GigabitEthernet1/0/0] quit
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk allow-pass vlan 20
[SwitchC-GigabitEthernet1/0/1] quit
```

SwitchA 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname SwitchA
[SwitchA] vlan 100
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 1/0/0
[SwitchA-GigabitEthernet1/0/0] port vlan-stacking vlan 10 stack-vlan 100 !---配置内层 VLAN 10，外层 VLAN 100 的灵活 QinQ 功能
[SwitchA-GigabitEthernet1/0/0] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port vlan-stacking vlan 20 stack-vlan 100
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk allow-pass vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

（2）配置 QinQ 终结子接口支持 VRRP

在 RouterA 的子接口 GE2/0/0.1 上配置对外层 VLAN 100、内层 VLAN 10 的两层 Tag 报文的终结功能，创建 VRRP 备份组 1；在子接口 GE2/0/0.2 上配置对外层 VLAN 100、内层 VLAN 20 的两层 Tag 报文的终结功能，创建 VRRP 备份组 2。配置 RouterA 在两个备份组中的优先级均为 120，并配置抢占时间均为 20 s。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10    !---配置 GE2/0/0.1 子接口外层 VLAN 为 100，内层 VLAN 为 10
[RouterA-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterA-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10    !---配置外层 VLAN 100，内层 VLAN 10 的双层 Tag 终结子接口支持 VRRP 协议
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 100.1.1.111
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterA] interface gigabitethernet 2/0/0.2
[RouterA-GigabitEthernet2/0/0.2] qinq termination pe-vid 100 ce-vid 20
[RouterA-GigabitEthernet2/0/0.2] arp broadcast enable
[RouterA-GigabitEthernet2/0/0.2] qinq vrrp pe-vid 100 ce-vid 20
[RouterA-GigabitEthernet2/0/0.2] vrrp vrid 2 virtual-ip 200.1.1.111
```

```
[RouterA-GigabitEthernet2/0/0.2] vrrp vrid 2 priority 120
[RouterA-GigabitEthernet2/0/0.2] vrrp vrid 2 preempt-mode timer delay 20
[RouterA-GigabitEthernet2/0/0.2] quit
```

在 RouterB 的子接口 GE2/0/0.1 上创建 VRRP 备份组 1，在子接口 GE2/0/0.2 上 VRRP 备份组 2，配置 RouterB 在两个备份组中的优先级均为缺省值，虚拟 IP 地址与 RouterA 上对应备份组中的虚拟 IP 地址相同。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[RouterB-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterB-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 100.1.1.111
[RouterB-GigabitEthernet2/0/0.1] quit
[RouterB] interface gigabitethernet 2/0/0.2
[RouterB-GigabitEthernet2/0/0.2] qinq termination pe-vid 100 ce-vid 20
[RouterB-GigabitEthernet2/0/0.2] arp broadcast enable
[RouterB-GigabitEthernet2/0/0.2] qinq vrrp pe-vid 100 ce-vid 20
[RouterB-GigabitEthernet2/0/0.2] vrrp vrid 2 virtual-ip 200.1.1.111
[RouterB-GigabitEthernet2/0/0.2] quit
```

完成上述配置以后，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可以看到 RouterA 在备份组中的状态均为 Master，RouterB 在备份组中的状态均为 Backup。下面是 RouterA 上的输出示例。

```
[RouterA] display vrrp
  GigabitEthernet2/0/0.1 | Virtual Router 1
    State : Master
    Virtual IP : 100.1.1.111
    Master IP : 100.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay time : 20 s
    TimerRun : 1
    TimerConfig : 1
    Auth type : NONE
    Virtual MAC :   0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-29 21:25:47
    Last change time : 2012-05-29 21:27:10

  GigabitEthernet2/0/0.2 | Virtual Router 2
    State : Master
    Virtual IP : 200.1.1.111
    Master IP : 200.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay time : 20 s
    TimerRun : 1
    TimerConfig : 1
    Auth type : NONE
    Virtual MAC :   0000-5e00-0102
    Check TTL : YES
```

```
Config type : normal-vrrp
Create time : 2012-05-29 21:25:47
Last change time : 2012-05-29 21:27:10
```

分别在 RouterA 和 RouterB 上执行 **display ip routing-table** 命令，RouterA 上可以看到路由表中有一条目的地址为虚拟 IP 地址的直连路由，而 RouterB 上该路由为 OSPF 路由，同样是因为当前 RouterA 为两个备份组中的 Master 设备，而 RouterB 为两个备份组中的 Backup 设备。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 16
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      100.1.1.0/24  Direct 0    0           D   100.1.1.1       GigabitEthernet2/0/0.1
      100.1.1.1/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
  100.1.1.111/32  Direct0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
      100.1.1.255/32Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF   10   2           D   100.1.1.2       GigabitEthernet2/0/0.1
                    OSPF   10   2           D   200.1.1.2       GigabitEthernet2/0/0.2
                    OSPF   10   2           D   192.168.2.2     GigabitEthernet1/0/0
    192.168.2.0/24  Direct 0    0           D   192.168.2.1     GigabitEthernet1/0/0
    192.168.2.1/32  Direct 0    0           D   127.0.0.1       GigabitEthernet1/0/0
    192.168.2.2/32  Direct 0    0           D   192.168.2.2     GigabitEthernet1/0/0
      200.1.1.0/24  Direct 0    0           D   200.1.1.1       GigabitEthernet2/0/0.2
      200.1.1.1/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.2
  200.1.1.111/32  Direct0    0           D   127.0.0.1       GigabitEthernet2/0/0.2
      200.1.1.255/32Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.2

[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 18
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      100.1.1.0/24  Direct 0    0           D   100.1.1.2       GigabitEthernet2/0/0.1
      100.1.1.2/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
  100.1.1.111/32  OSPF   10   2           D   100.1.1.1       GigabitEthernet2/0/0.1
                    OSPF   10   2           D   200.1.1.1       GigabitEthernet2/0/0.2
    100.1.1.255/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.1/32  Direct 0    0           D   127.0.0.1       GigabitEthernet1/0/0
    192.168.1.2/32  Direct 0    0           D   192.168.1.2     GigabitEthernet1/0/0
    192.168.2.0/24  OSPF   10   2           D   100.1.1.1       GigabitEthernet2/0/0.1
                    OSPF   10   2           D   200.1.1.1       GigabitEthernet2/0/0.2
                    OSPF   10   2           D   192.168.1.2     GigabitEthernet1/0/0
      200.1.1.0/24  Direct 0    0           D   200.1.1.2       GigabitEthernet2/0/0.2
      200.1.1.2/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.2
  200.1.1.111/32  OSPF   10   2           D   100.1.1.1       GigabitEthernet2/0/0.1
                    OSPF   10   2           D   200.1.1.1       GigabitEthernet2/0/0.2
    200.1.1.255/32  Direct 0    0           D   127.0.0.1       GigabitEthernet2/0/0.1
```

在 RouterA 的接口 GE2/0/0.1 上执行 **shutdown** 命令，模拟链路故障。分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组 1 中的状态切换为 Initialize，RouterB 在备份组 1 中的状态切换为 Master。下面是 RouterA 上的输出示例。

```
[RouterA] display vrrp
  GigabitEthernet2/0/0.1 | Virtual Router 1
    State : Initialize
    Virtual IP : 100.1.1.111
    Master IP : 0.0.0.0
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 0
    Preempt : YES     Delay time : 20 s
    TimerRun : 1
    TimerConfig : 1
    Auth type : NONE
    Virtual MAC :   0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-29 21:27:47
    Last change time : 2012-05-29 21:29:10

  GigabitEthernet2/0/0.2 | Virtual Router 2
    State : Master
    Virtual IP : 200.1.1.111
    Master IP : 200.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay time : 20 s
    TimerRun : 1
    TimerConfig : 1
    Auth type : NONE
    Virtual MAC :   0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2012-05-29 21:25:47
    Last change time : 2012-05-29 21:27:10
```

在 RouterA 的接口 GE2/0/0.1 上执行 **undo shutdown** 命令，恢复链路故障。20 s 后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组 1 中的状态恢复为 Master，RouterB 在备份组 1 中的状态恢复为 Backup。输出示例略。

8.3 VRRP 联动功能配置与管理

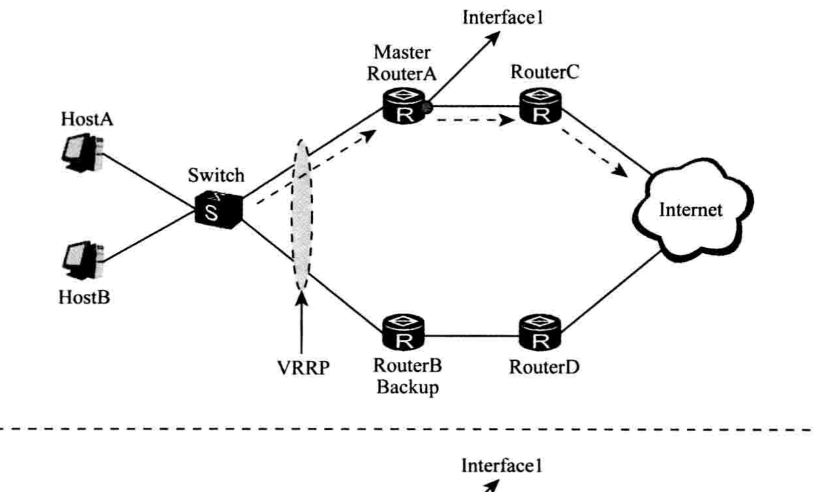
通过前面的学习，我们已经知道，可以利用 VRRP 实现网关设备的主备备份或者负载分担。但是 VRRP 备份组监控功能还存在一些不足：**一是仅能感知 VRRP 接口状态的变化，无法感知 VRRP 设备直连或者非直连上行链路状态**，导致用户业务流量的中断；二是当 Master 设备出现故障时，Backup 设备需要等待 Master_Down_Interval 后才能感知故障并切换为 Master 设备，且切换时间通常在 3 s 以上，无法满足一些业务量大的用户需求。

我们知道，正因为有了第 7 章介绍的 BFD 可以实现更快速的主备切换，接口状态跟踪、BFD、NQA，加上后面各章将要介绍的动态路由协议可以做到对这类链路的监控（参见 8.1.7 节介绍），所以结合这些技术可以实现 VRRP 备份组对设备直连或者非直连上行链路的监控。但在配置 VRRP 备份组联动功能之前，需完成上节介绍的 VRRP 基本功能配置。

8.3.1　配置 VRRP 与接口状态联动监视上行接口

VRRP 与接口状态联动监视上行接口方案是为了解决 VRRP 备份组只能感知其所在接口（**下行接口**）状态的变化，而无法感知 VRRP 设备上行接口或直连链路故障，导致业务流量中断的问题。**在 Master 设备上**部署了 VRRP 与接口状态联动监视上行接口功能后，当 Master 设备的上行接口或直连链路发生故障时，可通过调整自身优先级触发主备切换，确保流量正常转发。

如图 8-12 所示，RouterA 和 RouterB 之间配置了 VRRP 备份组，其中 RouterA 为 Master 设备，RouterB 为 Backup 设备，RouterA 和 RouterB 皆工作在抢占方式下。在担当 Master 设备的 RouterA 上配置以 Reduced 方式监视上行接口 Interface1，当 Interface1 故障时，RouterA 降低自身优先级，通过报文协商，RouterB 抢占成为 Master，确保用户流量正常转发。



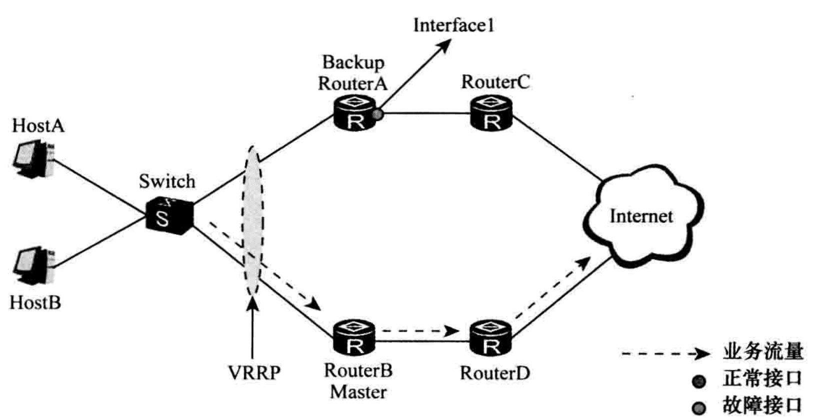


图 8-12　VRRP 监视上行接口的应用示例

说明 配置 VRRP 与接口状态联动时，备份组中的 Master 和 Backup 设备必须都工作在抢占方式下。建议 Backup 设备配置为立即抢占，Master 设备配置为延时抢占，这样当被监视的接口故障恢复时，**原 Master 设备在备份组中的优先级将恢复原来的值，能重新抢占成为 Master**，继续承担流量转发的业务。

配置 VRRP 与接口状态联动监视上行接口的步骤如表 8-7 所示（**仅可在 Master 设备上配置**）。

表 8-7　**VRRP 与接口状态联动监视上行接口的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入 **Master 设备 VRRP 接口**，可以是物理接口、逻辑接口或者子接口，进入接口视图
3	**vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *value-reduced*] 例如：[Huawei-GigabitEthernet1/0/0]**vrrp vrid** 1 **track interface** gigabitethernet 2/0/0 **reduced** 50	配置 VRRP 备份组与上行接口状态联动。命令中的参数说明如下 ● *virtual-router-id*：指定要配置与接口状态联动的 VRRP 备份组号 ● *interface-type interface-number*：指定要监视状态的上行接口 ● **reduced** *value-reduced*：可选参数，指定当被监视的上行接口状态变为 Down 时，Master 设备优先级降低的数值（**不是指降低后的优先级值**），取值范围为 1～255 的整数。优先级最低可以降至 1，**但必须确保优先级降低后 Master 设备的优先级低于当前 Backup 设备的优先级（值越大，优先级越高），以触发主备切换**。如果不选择此可选参数，则降低值为缺省值。缺省情况下，当被监视的接口变为 Down 时，优先级的数值降低 10 【注意】当设备为 IP 地址拥有者，即当采用该设备 VRRP 接口 IP 地址作为虚拟路由器的 IP 地址时，不允许对该设备配置监视接口，因为此时该设备总是 Master。多个 VRRP 备份组可以监视同一个上行接口，一个 VRRP 备份组最多可以同时监视 8 个上行接口 缺省情况下，未使能 VRRP 通过监视接口的状态实现主备快速切换的功能，可用 **undo vrrp vrid** *virtual-router-id* **track interface** [*interface-type interface-number*] 命令去使能指定 VRRP 备份组通过监视上行接口的状态实现主备快速切换的功能

8.3.2 配置 VRRP 与 BFD 联动实现快速切换

VRRP 与 BFD 联动实现快速切换功能是为了解决 VRRP 备份组在 Master 设备出现故障时，Backup 设备需要等待 Master_Down_Interval 定时器确定的时长（通常在 3 s 以上）后才能感知故障并切换为 Master 设备，导致业务数据丢失的问题。

通过在 Master 设备和 Backup 设备之间（通过下行链路）建立 BFD 会话，并在

Backup 设备上与 VRRP 备份组进行绑定，就能快速地检测 **VRRP 备份组设备之间的连通状态**，并在出现故障时及时通知 VRRP 备份组以实现毫秒级的快速切换，减少流量丢失。

如图 8-13 所示，RouterA 和 RouterB 之间配置 VRRP 备份组，RouterA 为 Master 设备，RouterB 为 Backup 设备，用户侧的流量通过 RouterA 转发。RouterA 和 RouterB 皆工作在抢占方式下，其中 RouterB 为立即抢占。在 RouterA 和 RouterB 两端配置 BFD 会话，并在 RouterB 上配置 VRRP 与 BFD 联动。当 RouterB 与 RouterA 之间出现链路故障时，BFD 快速检测故障并通知 RouterB 增加指定的优先级（**此时 RouterB 的优先级需高于 RouterA 的优先级**），RouterB 立即抢占为 Master，用户侧流量通过 RouterB 转发，实现了主备的快速切换。

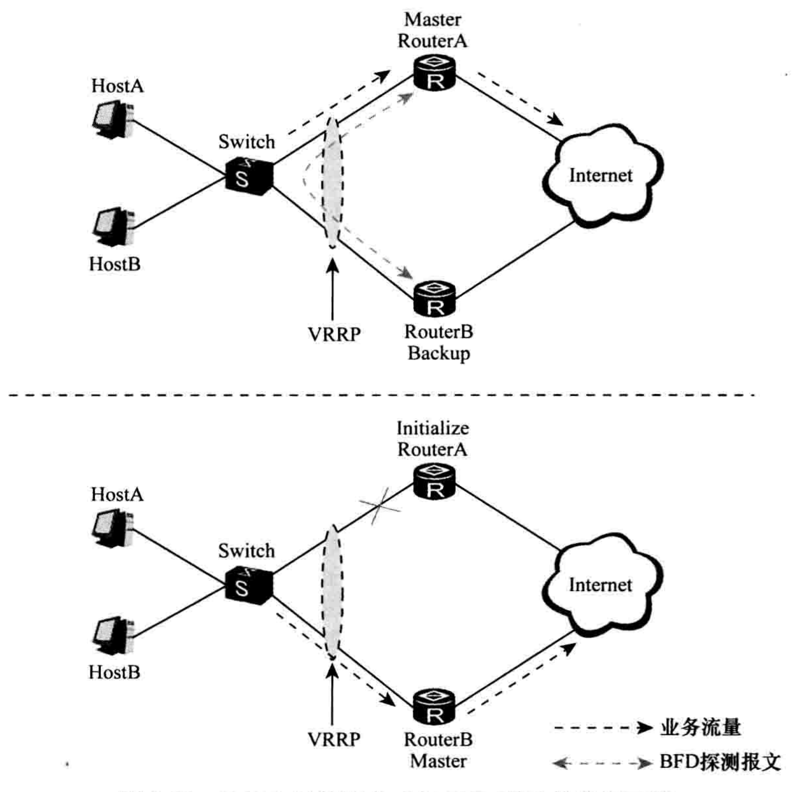


图 8-13　VRRP 以普通方式与 BFD 联动的应用示例

说明　VRRP 与 BFD 联动**仅支持与静态的 BFD 会话类型或静态标识符自协商的 BFD 会话类型的联动**。配置 VRRP 与 BFD 联动时，备份组中的 **Master 和 Backup 设备必须都工作在抢占方式下**。建议 Backup 设备配置为立即抢占，Master 设备配置为延时抢占，**以实现在 VRRP 备份组故障恢复时 Backup 设备在备份组中的优先级恢复为原来的值，原 Master 设备能重新抢占成为** Master，继续承担流量转发的业务。有关 BFD 的相关知识请参见本书第 7 章。

VRRP 与 BFD 联动的具体配置步骤如表 8-8 所示（**仅可在 Backup 设备上配置**）。

表 8-8 **VRRP 与 BFD 联动实现快速切换的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入 **Backup 设备 VRRP 接口**，可以是物理接口、逻辑接口或者子接口，进入接口视图
3	**vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased*] 例如：Huawei-GigabitEthernet1/0/0] **vrrp vrid 1 track bfd-session 1 increased** 40	在 Backup 设备 VRRP 接口上使能 VRRP 通过联动 BFD 会话状态来实现快速主备切换的功能。命令中的参数说明如下 ● *virtual-router-id*：指定要配置与 BFD 联动的 VRRP 备份组号 ● *bfd-session-id*，二选一参数，指定被监视的 BFD 会话的本地标识符，取值范围为 1～8 191 的整数 ● **session-name** *bfd-configure-name*：二选一参数，指定被监视的 BFD 会话的名称，1～15 个字符，不支持空格，不区分大小写 ● **increased** *value-increased*：可选参数，指定当被监视的 BFD 会话状态变为 Down 时，Backup 设备优先级增加的数值（**不是指增加后的优先级值**），取值范围是 1～253，增加后的优先级最高只能达到 254，**但必须确保优先级增加后 Backup 设备的优先级高于当前 Master 设备的优先级，以触发主备切换** 【注意】当 VRRP 备份组中存在 IP 地址拥有者时，不允许对其配置监视 BFD 会话功能，因为 IP 地址拥有者将始终成为 Master。如果选择参数 **session-name** *bfd-configure-name*，则只能绑定静态标识符自协商的 BFD 会话类型；如果选择参数 *bfd-session-id*，则只能绑定静态的 BFD 会话类型 缺省情况下，未使能 VRRP 通过监视 BFD 会话状态实现快速主备切换的功能，可用 **undo vrrp vrid** *virtual-router-id* **track interface** [*interface-type interface-number*]命令去使能指定 VRRP 备份组通过监视指定 BFD 会话状态实现快速主备切换的功能

8.3.3 配置 VRRP 与 BFD/NQA/路由联动监视上行链路

VRRP 与 BFD/NQA/路由联动监视上行链路也是为了解决 VRRP 不能感知 Master 设备上行非直连链路故障，导致用户流量丢失的问题。**通过在 Master 设备上配置 BFD/NQA/路由检测 Master 上行链路的连通状况**，当 Master 设备的上行链路发生故障时，BFD/NQA/路由可以快速检测故障并通知 Master 设备调整自身优先级，触发主备切换，确保流量正常转发。

如图 8-14 所示，RouterA 和 RouterB 之间配置了 VRRP 备份组，其中 RouterA 为 Master 设备，RouterB 为 Backup 设备，RouterA 和 RouterB 皆工作在抢占方式下。配置 BFD/NQA/路由监测 RouterA 到 RouterE 之间的链路，并在 RouterA 上配置 VRRP 与 BFD/NQA/路由联动。当 BFD/NQA/路由检测到 RouterA 到 RouterE 之间的链路故障时，通知 RouterA 降低自身优先级，触发主备切换以实现链路切换，减小链路故障对业务转

发的影响。当上行链路故障恢复时，原 Master 设备在备份组中的优先级将恢复为原来的值，重新抢占成为 Master，继续承担流量转发的业务。

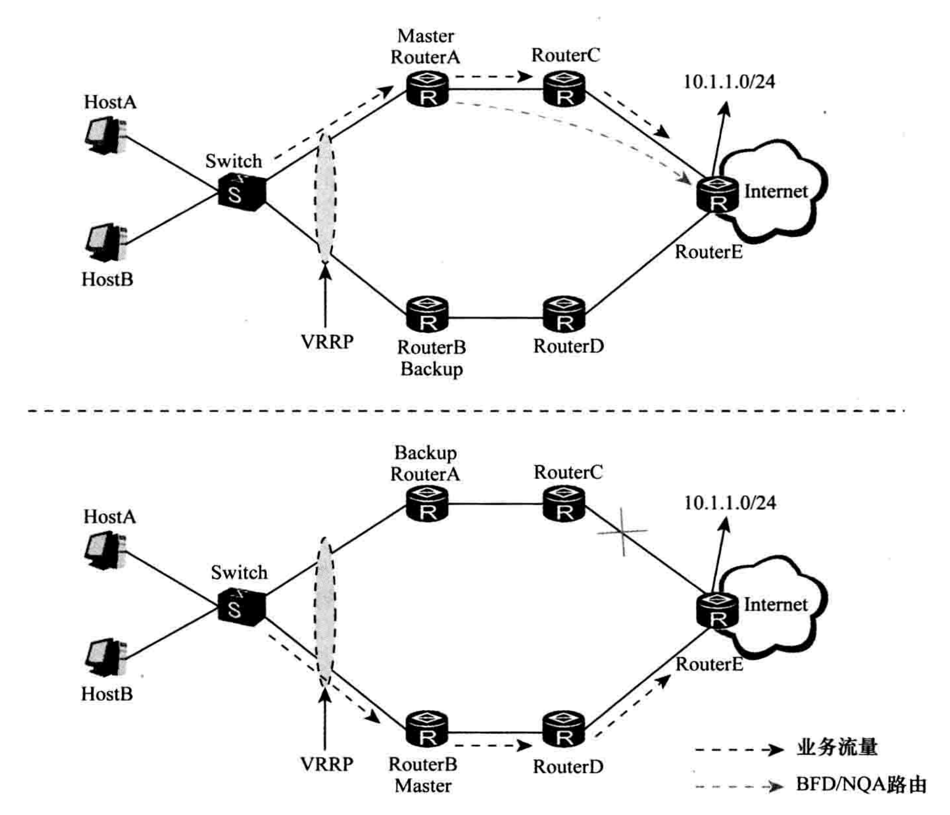


图 8-14　VRRP 与 BFD/NQA/路由联动监视上行链路的应用示例

说明　配置 VRRP 与 BFD/NQA/路由联动时，备份组中的 Master 和 Backup 设备必须都工作在抢占方式下。建议 Backup 设备配置为立即抢占，Master 设备配置为延时抢占，以实现在上行链路故障恢复时，**原 Master 设备在备份组中的优先级恢复为原来的值**，重新抢占成为 Master，继续承担流量转发的业务。

BFD 可以实现毫秒级的故障检测，联动 BFD 可以快速地检测故障，从而使主备切换速度更快，但仅支持联动静态和静态标识符自协商类型的 BFD 会话。

NQA 可以对响应时间、网络抖动、丢包率等网络信息进行统计，通过配置 NQA 测试失败百分比，联动 NQA 还可以实现在上行链路质量较差时触发主备切换，但仅支持联动 ICMP 类型的 NQA 测试例。

联动路由时的链路切换时间依赖于 VRRP 所联动路由协议的收敛速度，且 VRRP 与静态路由联动时仅能检测 Master 设备上行直连链路的故障，如需检测 Master 上行非直连链路的故障，请配置 VRRP 与动态路由联动。

VRRP 与 BFD/NQA/路由联动监视上行链路的具体配置步骤如表 8-9 所示（**仅可在 Master 设备上配置**）。有关 BFD 和 NQA 的具体配置方法参见本书第 7 章，下同。

表 8-9 **VRRP 与 BFD/NQA/路由联动监视上行链路的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interfa-ce-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入 **Master 设备 VRRP 接口**，可以是物理接口、逻辑接口或者子接口，进入接口视图
3	**vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name*} [**reduced** *value-reduced*] 例如：Huawei-GigabitEthernet1/0/0] **vrrp vrid 1 track bfd-session 1 reduced** 40	（三选一）在 Master 设备 VRRP 接口上使能 VRRP 通过联动 BFD 会话状态来实现主备切换的功能 可选参数 **reduced** *value-reduced* 用来指定当被监视的上行链路不可达时，Master 设备优先级降低的数值（**不是指降低后的优先级值**），取值范围为 1～255 的整数。优先级最低可以降至 1，**但必须确保优先级降低后 Master 设备的优先级低于当前 Backup 设备的优先级，以触发主备切换**。如果不选择此可选参数，则降低值为缺省值。缺省情况下，当被监视的接口变为 Down 时，优先级的数值降低 10。其他说明参见上节表 8-8 第 3 步 【注意】当 VRRP 备份组中存在 IP 地址拥有者时，不允许对其配置与 BFD 联动功能，因为 IP 地址拥有者将始终成为 Master
	vrrp vrid *virtual-router-id* **track nqa** *admin-name test-name* [**reduced** *value-reduced*] 例如：[Huawei-GigabitEthernet0/0/1] **vrrp vrid 1 track nqa** user user1 **reduced** 20	（三选一）在 Master 设备 VRRP 接口上使能 VRRP 与 NQA 联动功能。命令中的参数说明如下 • **vrid** *virtual-router-id*：指定配置 VRRP 与 NQA 联动的虚拟路由器编号，取值范围为 1～255 的整数 • *admin-name*：创建用于与 VRRP 联动的 NQA 测试实例管理员账户名称，1～32 个字符，不支持空格，**区分大小写** • *test-name*：指定要与 VRRP 联动的 NQA 测试实例名（必须先创建 ICMP 类型的 NQA 测试例，本书不作介绍，可参见本章后面介绍的示例） • **reduced** *value-reduced*：可选参数，指定当被监视的 NQA 实例探测到上行链路不可达时，优先级降低的数值（**不是指降低后的优先级值**），取值范围为 1～255 的整数。优先级最低可以降至 1，缺省情况下，当被监视的 NQA 实例探测到上行链路不可达时，优先级的数值降低 10。**必须确保优先级降低后 Master 设备的优先级低于当前 Backup 设备的优先级，以触发主备切换** 【注意】当 VRRP 备份组中存在 IP 地址拥有者时，不允许对其配置与 NQA 联动功能，因为 IP 地址拥有者将始终成为 Master。VRRP 备份组只能监视 ICMP 类型的 NQA 测试例。VRRP 备份组最多可同时监视 8 个 NQA 实例 缺省情况下，未使能 VRRP 备份监视 NQA 实例状态实现主备切换功能，可用 **undo vrrp vrid** *virtual-router-id* **track nqa** [*admin-name test-name*]命令去使能指定 VRRP 备份组通过监视指定 NQA 实例的状态来实现主备切换功能
	vrrp vrid *virtual-router-id* **track ip route** *ip-address* { *mask-addre-ss* | *mask-length* } [**vpn-instance** *vpn-instance-name*] [**reduced** *value-reduced*]	（三选一）在 Master 设备 VRRP 接口上使能 VRRP 联动指定的路由功能。命令中的参数说明如下 • **vrid** *virtual-router-id*：指定配置 VRRP 与路由联动的虚拟路由器编号，取值范围为 1～255 的整数 • *ip-address*：指定被监控的路由的 IP 地址（**指被监控链路所在网络的网络 IP 地址**，不是具体接口 IP 地址）

（续表）

步骤	命令	说明
3	**vrrp vrid** *virtual-router-id* **track ip route** *ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*] [**reduced** *value-reduced*]	• { *mask-address* | *mask-length* }：指定被监控的路由的 IP 地址所对应的子网掩码或子网掩码长度 • **vpn-instance** *vpn-instance-name*：可选参数，指定被监控路由所在的 VPN 实例的名称，1～31 个字符，不支持空格，区分大小写 • **reduced** *value-reduced*：可选参数，指定当被监控的路由被撤销或变为非活跃状态时，优先级降低的数值（**不是降低后的优先级值**），取值范围为 1～255 的整数。优先级最低可以降至 1，缺省情况下，当被监控的路由被撤销或为非活跃状态时，优先级的数值降低 10。**必须确保优先级降低后 Master 设备的优先级低于当前 Backup 设备的优先级，以触发主备切换** 【注意】当 VRRP 备份组中存在 IP 地址拥有者时，不允许对其配置与路由联动功能，因为 IP 地址拥有者将始终成为 Master。当通过指定 VPN 实例设置 VRRP 监视路由功能时：如果指定的 VPN 实例不存在，则 VRRP 监视该 VPN 路由的配置将无法生效；如果在该功能配置成功后删除对应的 VPN 实例，则 VRRP 监视该 VPN 路由的配置将删除 缺省情况下，VRRP 监控路由功能未使能，可用 **undo vrrp vrid** *virtual-router-id* **track ip route** [*ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*]] 命令去使能指定 VRRP 备份组与指定路由的联动功能

配置好 VRRP 联动功能后，可以按照 8.2.5 小节介绍的管理命令检查 VRRP 配置，验证配置结果，或者清除 VRRP 报文统计信息。

8.3.4 VRRP 与接口状态联动监视上行接口的配置示例

本示例的基本拓扑结构如图 8-15 所示，局域网主机通过 Switch 双线连接到部署了 VRRP 备份组的 RouterA 和 RouterB，其中 RouterA 为 Master。现用户希望当 RouterA 的上行接口 GE1/0/0 状态 Down 时，VRRP 备份组能够及时感知并进行主备切换，由 RouterB 接替作为网关继续承担业务转发，以减小接口状态 Down 对业务传输的影响。

1. 基本配置思路分析

本示例要监控的是 RouterA 的上行接口，故可采用 VRRP 与接口状态联动来实现对上行接口故障的感知及主备网关的切换。其基本的配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

② 在 RouterA 和 RouterB 上配置 VRRP 备份组。其中，RouterA 上配置较高优先级，作为 Master 设备承担业务转发；RouterB 上配置较低优先级，作为 Backup 设备。

③ 在担当 Master 设备的 RouterA 上配置 VRRP 与接口状态联动，监视上行接口 GE1/0/0，实现在 RouterA 到 RouterC 间链路出现故障时，VRRP 备份组及时感知并进行主备切换的目的。

2. 具体配置步骤

（1）配置设备间的网络互连

首先配置设备各接口的 IP 地址，以 RouterA 为例。RouterB 和 RouterC 的配置与之类似，略。

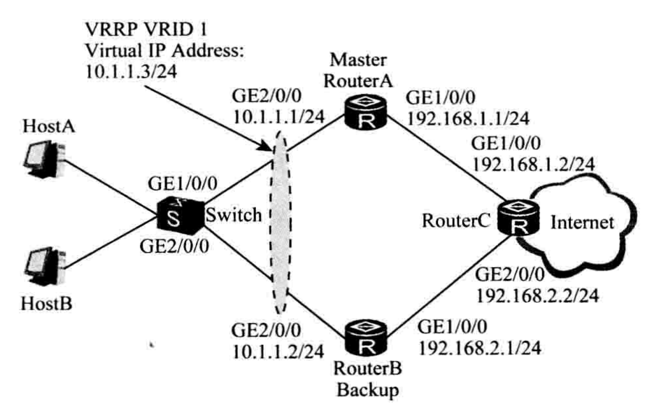


图 8-15 VRRP 与接口状态联动监视上行接口配置示例拓扑结构

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

然后配置 RouterA、RouterB 和 RouterC 间采用 OSPF 协议进行互连。以 RouterA 为例，RouterB 和 RouterC 的配置与之类似，略。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

（2）配置 VRRP 备份组

在 RouterA 上创建 VRRP 备份组 1，配置 RouterA 在该备份组中的优先级为 120，并配置抢占延时为 20 s。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.3
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet2/0/0] quit
```

在 RouterB 上创建 VRRP 备份组 1，其在该备份组中的优先级为缺省值 100。

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.3
[RouterB-GigabitEthernet2/0/0] quit
```

（3）配置 VRRP 与接口状态联动

在 RouterA 上配置 VRRP 与接口状态联动，当监视的接口 GE1/0/0 状态 Down 时，RouterA 的优先级降低 40（这时原来 Master 设备 RouterA 的优先级就为 80，低于原来 Backup 设备 RouterB 的优先级，可使 RouterB 切换为 Master 状态）。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 track interface gigabitethernet 1/0/0 reduced 40
[RouterA-GigabitEthernet2/0/0] quit
```

完成上述配置后，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可以看到 RouterA 为 Master 设备，联动的接口状态为 Up，RouterB 为 Backup 设备。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State              : Master
    Virtual IP         : 10.1.1.3
    Master IP          : 10.1.1.1
    PriorityRun        : 120
    PriorityConfig     : 120
    MasterPriority     : 120
    Preempt            : YES     Delay Time : 20 s
    TimerRun           : 1 s
    TimerConfig        : 1 s
    Auth Type          : NONE
    Virtual Mac        :   0000-5e00-0101
    Check TTL          : YES
    Config type : normal-vrrp
    Track IF           : GigabitEthernet1/0/0     Priority reduced : 40
    IF state           : UP
    Create time        : 2012-05-22 17:32:56
    Last change time : 2012-05-22 17:33:00
```

在 RouterA 的接口 GE1/0/0 上执行 **shutdown** 命令模拟链路故障，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可以看到 RouterA 状态切换成 Backup，联动的接口状态为 Down，RouterB 的状态切换为 Master，证明配置是成功的。下面是 RouterB 上的输出示例。

```
<RouterB> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State              : Master
    Virtual IP         : 10.1.1.3
    Master IP          : 10.1.1.2
    PriorityRun        : 100
    PriorityConfig     : 100
    MasterPriority     : 100
    Preempt            : YES     Delay Time : 0 s
    TimerRun           : 1 s
    TimerConfig        : 1 s
    Auth Type          : NONE
    Virtual Mac        :   0000-5e00-0101
    Check TTL          : YES
    Config type        : normal-vrrp
    Create time        : 2012-05-22 17:34:00
    Last change time : 2012-05-22 17:34:04
```

然后在 RouterA 的接口 GE1/0/0 上执行 **undo shutdown** 命令恢复链路故障，再在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，20 s 后，可以看到 RouterA 状态恢复为 Master，联动的接口状态为 Up，RouterB 的状态恢复为 Backup。输出示例略。

8.3.5 VRRP 与 BFD 联动实现快速切换配置示例

本示例的基本拓扑结构如图 8-16 所示，局域网内的主机通过 Switch 双线连接到部署了 VRRP 备份组的 RouterA 和 RouterB，其中 RouterA 为 Master。用户希望当 RouterA 或 RouterA 到 Switch 间链路出现故障时，主备网关间的切换时间小于 1 s，以减少故障对业务传输的影响。

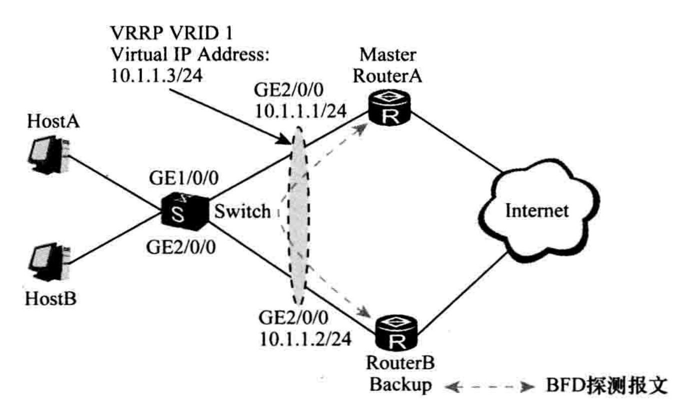


图 8-16 VRRP 与 BFD 联动实现快速切换配置示例拓扑结构

1. 基本配置思路分析

本示例要监控的是 RouterA 和 RouterB 之间的链路状态，故需采用 VRRP 与 BFD 联动实现主备网关间的快速切换。其基本配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

② 在 RouterA 和 RouterB 上配置 VRRP 备份组，其中 RouterA 的优先级为 120，抢占延时为 20 s，作为 Master 设备；RouterB 的优先级为缺省值，作为 Backup 设备。

③ 在 RouterA 和 RouterB 上配置静态 BFD 会话，监测备份组之间的链路。

④ 在 RouterB 上配置 VRRP 与 BFD 联动，实现链路故障时 VRRP 备份组快速切换。

2. 具体配置步骤

① 配置设备各接口的 IP 地址，以 RouterA 为例。RouterB 的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

② 配置 VRRP 备份组

在 RouterA 上创建 VRRP 备份组 1，配置 RouterA 在该备份组中的优先级为 120，并配置抢占延时为 20 s。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.3
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet1/0/0] quit
```

在 RouterB 上创建 VRRP 备份组 1，其在该备份组中的优先级为缺省值 100。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.3
[RouterB-GigabitEthernet1/0/0] quit
```

③ 在 RouterA 和 RouterB 上分别配置 RouterA 与 RouterB 之间的静态 BFD 会话。有关静态 BFD 会话的配置步骤参见本书第 7 章。

```
[RouterA] bfd    !---全局使能 BFD 功能
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 10.1.1.2 interface gigabitethernet 2/0/0   !---创建名为 atob 的 BFD 会话，绑定对端（即 RouterB 的 VRRP 接口 IP 地址）和出接口（RouterA 的 VRRP 接口）
[RouterA-bfd-session-atob] discriminator local 1          !---配置本地标识符为 1
[RouterA-bfd-session-atob] discriminator remote 2         !---配置对端标识符为 2
[RouterA-bfd-session-atob] min-rx-interval 50             !---配置最大 BFD 会话报文的接收时间间隔为 50 ms
[RouterA-bfd-session-atob] min-tx-interval 50             !---配置最大 BFD 会话报文的发送时间间隔为 50 ms
[RouterA-bfd-session-atob] commit                         !---提交 BFD 会话配置
[RouterA-bfd-session-atob] quit
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip 10.1.1.1 interface gigabitethernet 2/0/0
[RouterB-bfd-session-btoa] discriminator local 2
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] min-rx-interval 50
[RouterB-bfd-session-btoa] min-tx-interval 50
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置完成后，在 RouterA 或 RouterB 上分别执行 **display bfd session** 命令，可以看到 BFD 会话的状态为 Up。下面是 RouterA 的输出示例，从可以看出 BFD 会话已建立（呈 Up 状态）。

```
<RouterA> display bfd session all
--------------------------------------------------------------------------------
Local Remote PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
1      2       10.1.1.2        Up        S_IP_IF     GigabitEthernet1/0/0
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

④ 在 Backup 设备 RouterB 上配置 VRRP 与 BFD 联动功能，当 BFD 会话状态 Down 时，RouterB 的优先级增加 40。

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 2 increased 40
[RouterB-GigabitEthernet1/0/0] quit
```

完成上述配置后，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可以看出 RouterA 为 Master 设备，RouterB 为 Backup 设备，联动的 BFD 会话状态为 Up。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.3
    Master IP        : 10.1.1.1
    PriorityRun      : 120
    PriorityConfig   : 120
    MasterPriority   : 120
    Preempt          : YES    Delay Time : 20 s
```

```
    TimerRun          : 1 s
    TimerConfig       : 1 s
    Auth Type         : NONE
    Virtual Mac       :  0000-5e00-0101
    Check TTL         : YES
    Config type       : normal-vrrp
    Create time       : 2012-05-22 17:32:56
    Last change time : 2012-05-22 17:33:00
```

在 RouterA 的接口 GE2/0/0 上执行 **shutdown** 命令，模拟链路故障。此时再在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可以看出 RouterA 状态变为 Initialize，RouterB 状态变为 Master，联动的 BFD 会话状态为 Down。输出示例如下。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State             : Initialize
    Virtual IP        : 10.1.1.3
    Master IP         : 0.0.0.0
    PriorityRun       : 120
    PriorityConfig    : 120
    MasterPriority    : 0
    Preempt           : YES    Delay Time : 20 s
    TimerRun          : 1 s
    TimerConfig       : 1 s
    Auth Type         : NONE
    Virtual Mac       :  0000-5e00-0101
    Check TTL         : YES
    Config type       : normal-vrrp
    Create time       : 2012-05-22 17:32:56
    Last change time : 2012-05-22 17:33:06
<RouterB> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State             : Master
    Virtual IP        : 10.1.1.3
    Master IP         : 10.1.1.2
    PriorityRun       : 140
    PriorityConfig    : 100
    MasterPriority    : 140
    Preempt           : YES    Delay Time : 0 s
    TimerRun          : 1 s
    TimerConfig       : 1 s
    Auth Type         : NONE
    Virtual Mac       :  0000-5e00-0101
    Check TTL         : YES
    Config type       : normal-vrrp
    Track BFD         : 2   Priority increased : 40
    BFD-Session State: DOWN
    Create time       : 2012-05-22 17:33:00
    Last change time : 2012-05-22 17:33:06
```

再在 RouterA 的接口 GE2/0/0 上执行 **undo shutdown** 命令，模拟故障恢复。20 s 后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看出 RouterA 状态恢复为 Master，RouterB 状态恢复为 Backup，联动的 BFD 会话状态恢复为 Up。输出示例如下。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State             : Master
```

```
    Virtual IP          : 10.1.1.3
    Master IP           : 10.1.1.1
    PriorityRun         : 120
    PriorityConfig      : 120
    MasterPriority      : 120
    Preempt             : YES    Delay Time : 20 s
    TimerRun            : 1 s
    TimerConfig         : 1 s
    Auth Type           : NONE
    Virtual Mac         :  0000-5e00-0101
    Check TTL           : YES
    Config type         : normal-vrrp
    Create time         : 2012-05-22 17:32:56
    Last change time : 2012-05-22 17:33:50
<RouterB> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State               : Backup
    Virtual IP          : 10.1.1.3
    Master IP           : 10.1.1.1
    PriorityRun         : 100
    PriorityConfig      : 100
    MasterPriority      : 120
    Preempt             : YES    Delay Time : 0 s
    TimerRun            : 1 s
    TimerConfig         : 1 s
    Auth Type           : NONE
    Virtual Mac         :  0000-5e00-0101
    Check TTL           : YES
    Config type         : normal-vrrp
    Track BFD           : 2   Priority increased : 40
    BFD-Session State: UP
    Create time         : 2012-05-22 17:33:00
    Last change time : 2012-05-22 17:33:50
```

8.3.6 VRRP 与 BFD 联动监视上行链路的配置示例

本示例的基本拓扑结构如图 8-17 所示，局域网内的主机通过 Switch 双归属到部署了 VRRP 备份组的 RouterA 和 RouterB，其中 RouterA 为 Master。正常情况下，RouterA 承担网关工作，用户侧流量经 Switch→RouterA→RouterC→RouterE 进行转发。用户希望当 RouterC 到 RouterE 之间的链路故障时，VRRP 备份组可以在 1 s 内感知故障，并快速进行主备切换，启用 RouterB 承担业务转发，以减小链路故障对业务转发的影响。

1. 基本配置思路分析

本示例监控的是上行**非直连链路**，可采用与 BFD 联动的方式，基本的配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

② 在 RouterA 和 RouterB 上配置 VRRP 备份组，其中 RouterA 的优先级为 120，抢占延时为 20 s，作为 Master 设备；RouterB 的优先级为缺省值，作为 Backup 设备。

③ 在 RouterA 和 RouterE 上配置静态 BFD 会话，监测 RouterA 到 RouterE 之间的链路。

④ 在 RouterA 上配置 VRRP 与 BFD 联动，实现链路故障时触发 VRRP 备份组主备切换的目的。

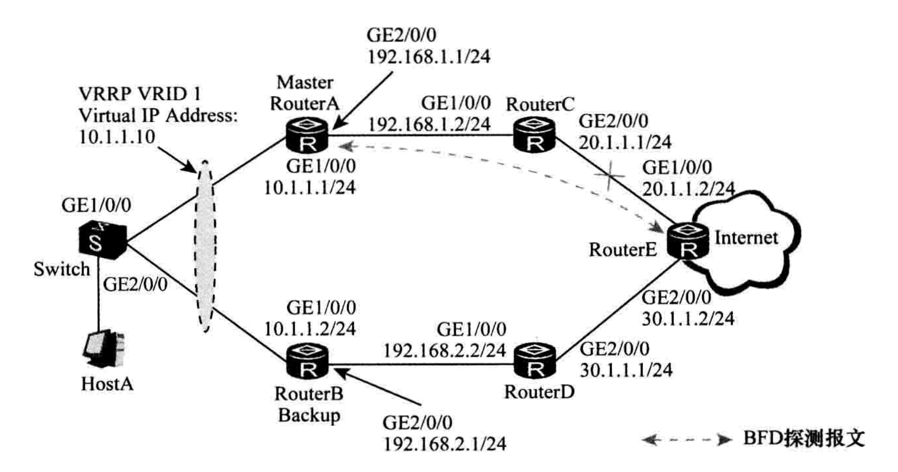


图 8-17 VRRP 与 BFD 联动监视上行链路配置示例的拓扑结构

2. 具体配置步骤

① 配置设备间的网络互连。先配置设备各路由器接口 IP 地址。在此仅以 RouterA 为例，其余设备的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

然后配置各路由器间采用 OSPF 协议进行互连。在此仅以 RouterA 为例，其余 Router 的配置类似，略。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

② 在 RouterA 和 RouterB 上分别创建 VRRP 备份组 1，配置 RouterA 在该备份组中的优先级为 120，并配置抢占时间为 20 s，RouterB 在该备份组中的优先级为缺省值 100。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.10
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.10
[RouterB-GigabitEthernet1/0/0] quit
```

③ 在 RouterA 和 RouterE 上分别配置它们之间的静态 BFD 会话。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atoe bind peer-ip 20.1.1.2
[RouterA-bfd-session-atoe] discriminator local 1
[RouterA-bfd-session-atoe] discriminator remote 2
```

```
[RouterA-bfd-session-atoe] min-rx-interval 50
[RouterA-bfd-session-atoe] min-tx-interval 50
[RouterA-bfd-session-atoe] commit
[RouterA-bfd-session-atoe] quit
[RouterE] bfd
[RouterE-bfd] quit
[RouterE] bfd etoa bind peer-ip 192.168.1.1
[RouterE-bfd-session-etoa] discriminator local 2
[RouterE-bfd-session-etoa] discriminator remote 1
[RouterE-bfd-session-etoa] min-rx-interval 50
[RouterE-bfd-session-etoa] min-tx-interval 50
[RouterE-bfd-session-etoa] commit
[RouterE-bfd-session-etoa] quit
```

④ 在 RouterA 上配置 VRRP 与 BFD 联动，当 BFD 会话状态 Down 时，RouterA 的优先级降低 40。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 1 reduced 40
[RouterA-GigabitEthernet1/0/0] quit
```

完成上述配置后，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可看出 RouterA 为 Master 设备， BFD 会话状态为 Up，RouterB 为 Backup 设备。以下是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State             : Master
    Virtual IP        : 10.1.1.10
    Master IP         : 10.1.1.1
    PriorityRun       : 120
    PriorityConfig    : 120
    MasterPriority    : 120
    Preempt           : YES    Delay Time : 20 s
    TimerRun          : 1 s
    TimerConfig       : 1 s
    Auth Type         : NONE
    Virtual Mac       :  0000-5e00-0101
    Check TTL         : YES
    Config type       : normal-vrrp
    Track BFD         : 1   Priority reduced : 40
    BFD-Session State: UP
    Create time       : 2012-05-22 17:32:56
    Last change time : 2012-05-22 17:33:00
```

在 RouterE 的接口 GE1/0/0 上执行 **shutdown** 命令，模拟链路故障。然后在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可看出 RouterA 状态切换为 Backup，联动的 BFD 会话状态变为 Down，RouterB 状态切换为 Master。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State             : Backup
    Virtual IP        : 10.1.1.10
    Master IP         : 10.1.1.2
    PriorityRun       : 80
    PriorityConfig    : 120
    MasterPriority    : 100
    Preempt           : YES    Delay Time : 20 s
```

```
        TimerRun              : 1 s
        TimerConfig           : 1 s
        Auth Type             : NONE
        Virtual Mac           :  0000-5e00-0101
        Check TTL             : YES
        Config type           : normal-vrrp
        Track BFD             : 1    Priority reduced : 40
        BFD-Session State: DOWN
        Create time           : 2012-05-22 17:34:56
        Last change time : 2012-05-22 17:35:00
```

再在 RouterE 的接口 GE1/0/0 上执行 **undo shutdown** 命令，恢复链路故障。20 s 后，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可看出 RouterA 状态恢复为 Master，联动的 BFD 会话状态恢复为 Up，RouterB 状态恢复为 Backup。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
        State                 : Master
        Virtual IP            : 10.1.1.10
        Master IP             : 10.1.1.1
        PriorityRun           : 120
        PriorityConfig        : 120
        MasterPriority        : 120
        Preempt               : YES     Delay Time : 20 s
        TimerRun              : 1 s
        TimerConfig           : 1 s
        Auth Type             : NONE
        Virtual Mac           :  0000-5e00-0101
        Check TTL             : YES
        Config type           : normal-vrrp
        Track BFD             : 1    Priority reduced : 40
        BFD-Session State: UP
        Create time           : 2012-05-22 17:36:56
        Last change time : 2012-05-22 17:37:00
```

8.3.7 VRRP 与 NQA 联动监视上行链路配置示例

如图 8-18 所示，局域网内的主机通过 Switch 双线连接到部署了 VRRP 备份组的 RouterA 和 RouterB，其中 RouterA 为 Master。正常情况下，RouterA 承担网关工作，用户侧流量由 Switch→RouterA→RouterC→RouterE 进行转发。用户希望当 RouterC 到 RouterE 之间的链路故障或链路质量较差时，VRRP 备份组可以感知并进行主备切换，启用 RouterB 承担业务转发，以减小链路故障对业务转发的影响。

1. 基本配置思路分析

本示例要监控非直连上行链路，可采用 VRRP 与 NQA 联动实现对上行链路故障的感知及主备网关的切换。其基本配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

② 在 RouterA 和 RouterB 上配置 VRRP 备份组，其中 RouterA 的优先级为 120，抢占延时为 20 s，作为 Master 设备；RouterB 的优先级为缺省值，作为 Backup 设备。

③ 在 RouterA 上配置 ICMP 类型的 NQA 测试例，配置目的地址为 RouterE 上接口

GE1/0/0 的 IP 地址，监测 RouterA 到 RouterE 的接口 GE1/0/0 间链路的连通性。

④ 在 RouterA 上配置 VRRP 和 NQA 联动，当 NQA 检测到链路故障时，触发 VRRP 备份组进行主备切换。

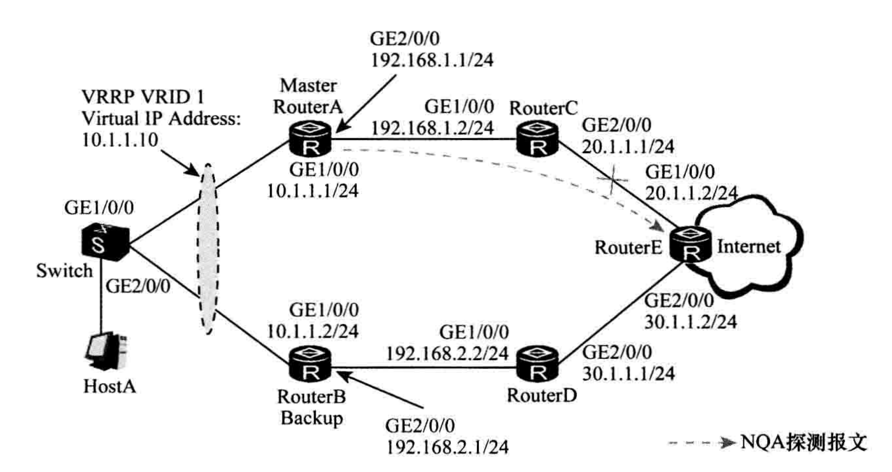


图 8-18　VRRP 与 NQA 联动监视上行链路配置示例的拓扑结构

2. 具体配置步骤

① 配置设备间的网络互连。先配置各路由器接口 IP 地址，在此仅以 RouterA 为例，其余路由器的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

然后配置各路由器间采用 OSPF 协议进行互连。在此仅以 RouterA 为例，其余路由器的配置类似，略。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

② 在 RouterA 和 RouterB 上分别创建 VRRP 备份组 1，配置 RouterA 在该备份组中的优先级为 120，并配置抢占时间为 20 s，RouterB 在该备份组中的优先级为缺省值 100。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.10
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 1/0/0
```

```
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.10
[RouterB-GigabitEthernet1/0/0] quit
```

③ 在 RouterA 上配置目的 IP 地址为 20.1.1.2/24 的 ICMP 类型的 NQA 测试例，当丢包率达到 80%时，判定测试例 failed（失败）。

```
[RouterA] nqa test-instance user test     !---创建管理者为 user，名为 test 的 NQA 测试例，并进入 NQA 测试例视图
[RouterA-user-test] test-type icmp        !---指定上述 NQA 测试例为 ICMP 测试
[RouterA-user-test] destination-address ipv4 20.1.1.2  !---配置上述 NQA 测试例的目的 IP 地址为 20.1.1.2（即 RouterE 与 RouterC 连接的接口 IP 地址）
[RouterA-user-test] frequency 20          !--- 配置上述 NQA 测试例自动执行测试的时间间隔为 20 秒
[RouterA-user-test] probe-count 5         !--- 配置 NQA 测试例的一次测试探针数目为 5
[RouterA-user-test] start now             !--- 立即启动执行上述 NQA 测试例
[RouterA-user-test] quit
```

④ 在 RouterA 配置 VRRP 与 NQA 联动功能，当 NQA 测试例 failed 时，RouterA 的优先级降低 40。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track nqa user test reduced 40
[RouterA-GigabitEthernet1/0/0] quit
```

完成上述配置后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 的状态为 Master，联动的 NQA 测试例状态为 success（成功），RouterB 的状态为 Backup。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State             : Master
    Virtual IP        : 10.1.1.10
    Master IP         : 10.1.1.1
    PriorityRun       : 120
    PriorityConfig    : 120
    MasterPriority    : 120
    Preempt           : YES    Delay Time : 20 s
    TimerRun          : 1 s
    TimerConfig       : 1 s
    Auth Type         : NONE
    Virtual Mac       :  0000-5e00-0101
    Check TTL         : YES
    Config type       : normal-vrrp
    Track NQA : user   test    Priority reduced : 40
    NQA state : success
    Create time       : 2012-05-22 17:32:56
    Last change time : 2012-05-22 17:33:00
```

在 RouterE 的接口 GE1/0/0 上执行 **shutdown** 命令，模拟链路故障。然后在 RouterA 上执行 **display nqa results test-instance** user test 命令，可以看到 NQA 测试实例的状态为 failed。

```
<RouterA> display nqa results test-instance user test
NQA entry(user, test) :testflag is active ,testtype is icmp
  1 .Test 1 result   The test is finished
   Send operation times: 5              Receive response times: 0
   Completion:failed                    RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:5
```

```
System busy operation number:0          Connection fail number:0
Operation sequence errors number:0      RTT Stats errors number:0
Destination ip address:20.1.1.2
Min/Max/Average Completion Time: 0/0/0
Sum/Square-Sum  Completion Time: 0/0
Last Good Probe Time: 0000-00-00 00:00:00.0
Lost packet ratio: 100 %
```

再分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 的状态切换为 Backup，联动的 NQA 测试例状态为 failed，RouterB 的状态切换为 Master。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State            : Backup
    Virtual IP       : 10.1.1.10
    Master IP        : 10.1.1.1
    PriorityRun      : 80
    PriorityConfig   : 120
    MasterPriority   : 100
    Preempt          : YES    Delay Time : 20 s
    TimerRun         : 1 s
    TimerConfig      : 1 s
    Auth Type        : NONE
    Virtual Mac      :  0000-5e00-0101
    Check TTL        : YES
    Config type      : normal-vrrp
    Track NQA : user   test    Priority reduced : 40
    NQA state : failed
    Create time      : 2012-05-22 17:34:56
    Last change time : 2012-05-22 17:35:00
```

在 RouterE 的接口 GE1/0/0 上执行 **undo shutdown** 命令，恢复链路故障。20 s 后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 的状态恢复为 Master，联动的 NQA 测试例状态恢复为 success，RouterB 的状态恢复为 Backup。下面是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.10
    Master IP        : 10.1.1.1
    PriorityRun      : 120
    PriorityConfig   : 120
    MasterPriority   : 120
    Preempt          : YES    Delay Time : 20 s
    TimerRun         : 1 s
    TimerConfig      : 1 s
    Auth Type        : NONE
    Virtual Mac      :  0000-5e00-0101
    Check TTL        : YES
    Config type      : normal-vrrp
    Track NQA : user   test    Priority reduced : 40
    NQA state : success
```

```
Create time        : 2012-05-22 17:36:56
Last change time : 2012-05-22 17:37:00
```

8.3.8 VRRP 与路由联动监视上行链路配置示例

本示例的基本拓扑结构如图 8-19 所示，局域网内的主机通过 Switch 双线连接到部署了 VRRP 备份组的 RouterA 和 RouterB，其中 RouterA 为 Master。正常情况下，RouterA 承担网关工作，用户侧流量经 Switch→RouterA→RouterC→RouterE 进行转发。用户希望当 RouterC 到 RouterE 之间路由撤销或者状态变为非激活时，VRRP 备份组能感知并进行主备切换，启用 RouterB 承担业务转发，以减小链路故障对业务转发的影响。

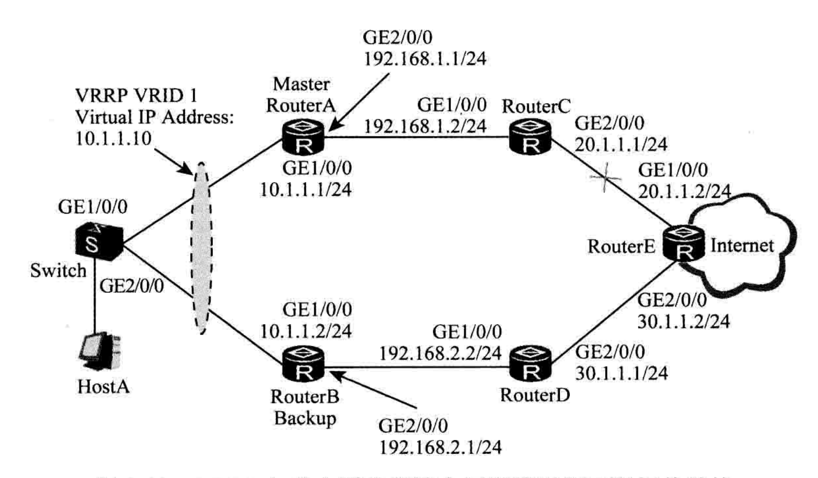


图 8-19 VRRP 与路由联动监视上行链路配置示例拓扑结构

1. 基本配置思路分析

本示例监控的对象是上行链路的路由，故可以采用 VRRP 与路由联动监视上行链路的方案。其基本配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

② 在 RouterA 和 RouterB 上配置 VRRP 备份组，其中，RouterA 上配置较高优先级和 20 s 抢占延时，作为 Master 设备承担流量转发；RouterB 上配置较低优先级，作为备用路由器。

③ 在 RouterA 上配置 VRRP 与路由联动功能，实现监控路由撤销或状态变为非激活时，触发 VRRP 备份组进行主备切换的目的。

2. 基本配置步骤

① 配置各路由器接口 IP 地址，以 RouterA 为例，其余路由器的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

② 在 RouterA 和 RouterB 上分别创建 VRRP 备份组 1，配置 RouterA 在该备份组中的优先级为 120，并配置抢占时间为 20 s，RouterB 在该备份组中的优先级为缺省值 100。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.10
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.10
[RouterB-GigabitEthernet1/0/0] quit
```

③ 配置 IS-IS 路由协议。以 RouterA、RouterC 和 RouterE 为例，其余路由器设备的配置与之类似，略。也可用 OSPF 等其他动态路由协议，有关 IS-IS 路由的配置方法将在本书后面介绍。

配置 RouterA 上 IS-IS 实体名称为 10.0000.0000.0001.00，级别为 1。

```
[RouterA] isis 1                                         !---创建 IS-IS 进程 1
[RouterA-isis-1] is-level level-1                        !---指定 RouterA 为 level-1 路由器
[RouterA-isis-1] network-entity 10.0000.0000.0001.00     !---配置 RouterA 的 IS-IS 实体名称为 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1             !---在 GE1/0/0 接口上使能 IS-IS 进程 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

配置 RouterC 上 IS-IS 实体名称为 10.0000.0000.0002.00。

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0002.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable 1
[RouterC-GigabitEthernet2/0/0] quit
```

配置 RouterE 上 IS-IS 实体名称为 10.0000.0000.0003.00 和 20.0000.0000.0003.00。

```
[RouterE] isis 1
[RouterE-isis-1] network-entity 10.0000.0000.0003.00
[RouterE-isis-1] quit
[RouterE] interface gigabitethernet 1/0/0
[RouterE-GigabitEthernet1/0/0] isis enable 1
[RouterE-GigabitEthernet1/0/0] quit
[RouterE] isis 2
[RouterE-isis-2] network-entity 20.0000.0000.0003.00
[RouterE-isis-2] quit
[RouterE] interface gigabitethernet 2/0/0
[RouterE-GigabitEthernet2/0/0] isis enable 2
[RouterE-GigabitEthernet2/0/0] quit
```

④ 在 RouterA 上配置 VRRP 与路由联动功能，当到达被监控链路所在网络的路由

（网络 IP 地址为 20.1.1.0/24）撤销时，RouterA 的优先级降低 40。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track ip route 20.1.1.0 24 reduced 40
[RouterA-GigabitEthernet1/0/0] quit
```

完成上述配置后，在 RouterA 上执行 **display isis route** 命令，可以看到存在一条去往 20.1.1.0/24 网段的路由。

```
<RouterA> display isis route

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

IPV4 Destination      IntCost     ExtCost ExitInterface     NextHop           Flags
-------------------------------------------------------------------------------
192.168.1.0/24          10          NULL      GE0/0/2         Direct            D/-/L/-
20.1.1.0/24             20          NULL      GE0/0/2         192.168.1.2       A/-/-/-
10.1.1.0/24             10          NULL      Vlanif18        Direct            D/-/L/-
10.1.1.10/32            10          NULL      Vlanif18        Direct            D/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set
```

分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 的状态为 Master，联动的路由状态为 Reachable（可达），RouterB 的状态为 Backup。以下是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State              : Master
    Virtual IP         : 10.1.1.10
    Master IP          : 10.1.1.1
    PriorityRun        : 120
    PriorityConfig     : 120
    MasterPriority     : 120
    Preempt            : YES    Delay Time : 20 s
    TimerRun           : 1 s
    TimerConfig        : 1 s
    Auth Type          : NONE
    Virtual Mac        :  0000-5e00-0101
    Check TTL          : YES
    Config type        : normal-vrrp
    Track IP route : 20.1.1.0/24   Priority reduced : 40
    IP route state : Reachable
    Create time : 2012-05-29 21:25:47
    Last change time : 2012-05-29 21:25:51
```

在 RouterE 的接口 GE1/0/0 上执行 **shutdown** 命令，模拟链路故障。然后在 RouterA 上执行 **display isis route** 命令，可以看到去往 20.1.1.0/24 网段的路由被撤销了。

```
<RouterA> display isis route

                         Route information for ISIS(1)
                         -----------------------------
```

```
                    ISIS(1) Level-1 Forwarding Table
                    --------------------------------

IPV4 Destination    IntCost    ExtCost ExitInterface    NextHop     Flags
-------------------------------------------------------------------------------
192.168.1.0/24      10         NULL    GE2/0/0          Direct      D/-/L/-
10.1.1.0/24         10         NULL    Vlanif18         Direct      D/-/L/-
10.1.1.10/32        10         NULL    Vlanif18         Direct      D/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set
```

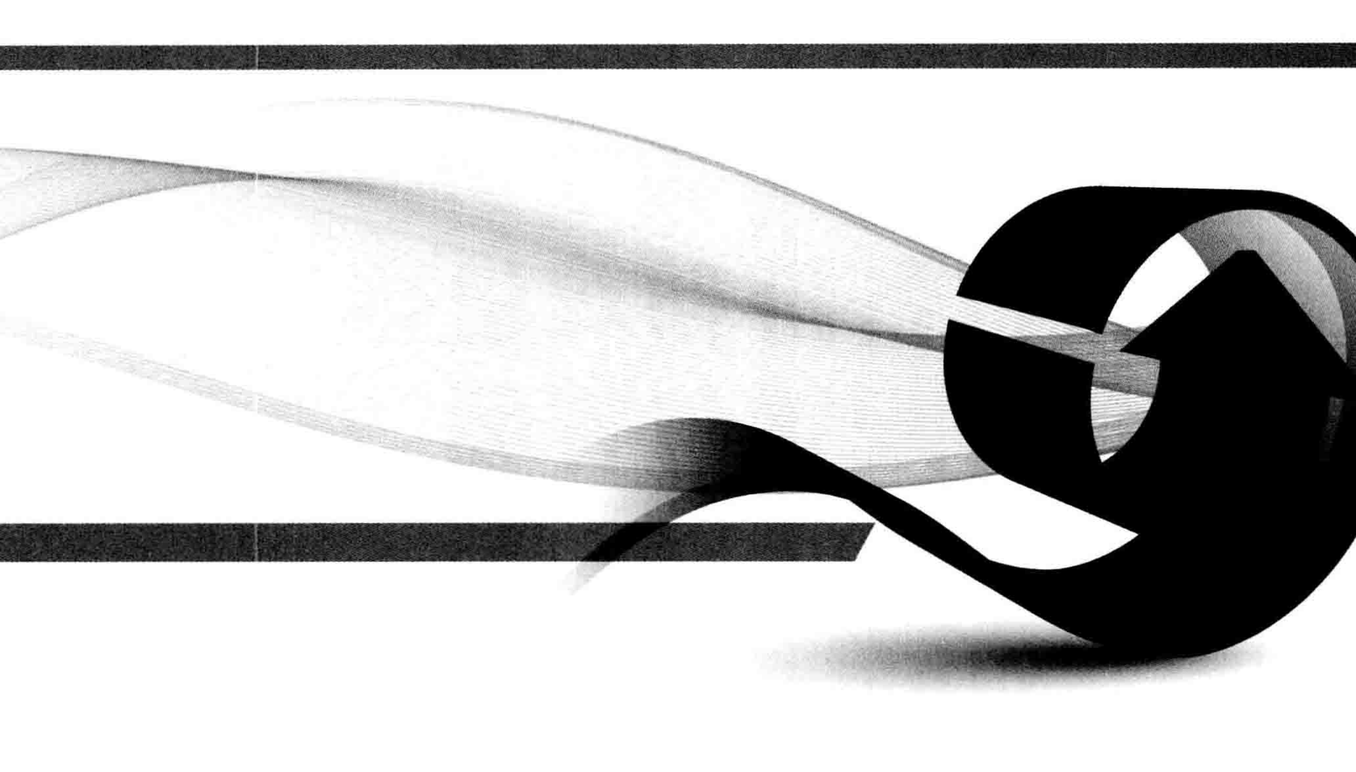
分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可看到 RouterA 的状态切换为 Backup，联动的路由状态为 Uneachable（不可达），RouterB 的状态切换为 Master。以下是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State            : Backup
    Virtual IP       : 10.1.1.10
    Master IP        : 10.1.1.2
    PriorityRun      : 80
    PriorityConfig   : 120
    MasterPriority   : 100
    Preempt          : YES     Delay Time : 20 s
    TimerRun         : 1 s
    TimerConfig      : 1 s
    Auth Type        : NONE
    Virtual Mac      :   0000-5e00-0101
    Check TTL        : YES
    Config type      : normal-vrrp
    Track IP route : 20.1.1.0/24    Priority reduced : 40
    IP route state : Unreachable
    Create time : 2012-05-29 21:25:47
    Last change time : 2012-05-29 21:25:51
```

在 RouterE 的接口 GE1/0/0 上执行 **undo shutdown** 命令，恢复链路故障。20s 后，分别在 RouterA 和 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 的状态恢复为 Master，联动的路由状态恢复为 Reachable，RouterB 的状态恢复为 Backup。以下是 RouterA 上的输出示例。

```
<RouterA> display vrrp
  GigabitEthernet1/0/0 | Virtual Router 1
    State            : Master
    Virtual IP       : 10.1.1.10
    Master IP        : 10.1.1.1
    PriorityRun      : 120
    PriorityConfig   : 120
    MasterPriority   : 120
    Preempt          : YES     Delay Time : 20 s
    TimerRun         : 1 s
    TimerConfig      : 1 s
    Auth Type        : NONE
    Virtual Mac      :   0000-5e00-0101
```

```
Check TTL          : YES
Config type        : normal-vrrp
Track IP route : 20.1.1.0/24    Priority reduced : 40
IP route state : Reachable
Create time : 2012-05-29 21:27:47
Last change time : 2012-05-29 21:27:51
```



第9章
接口备份和双机热备份配置与管理

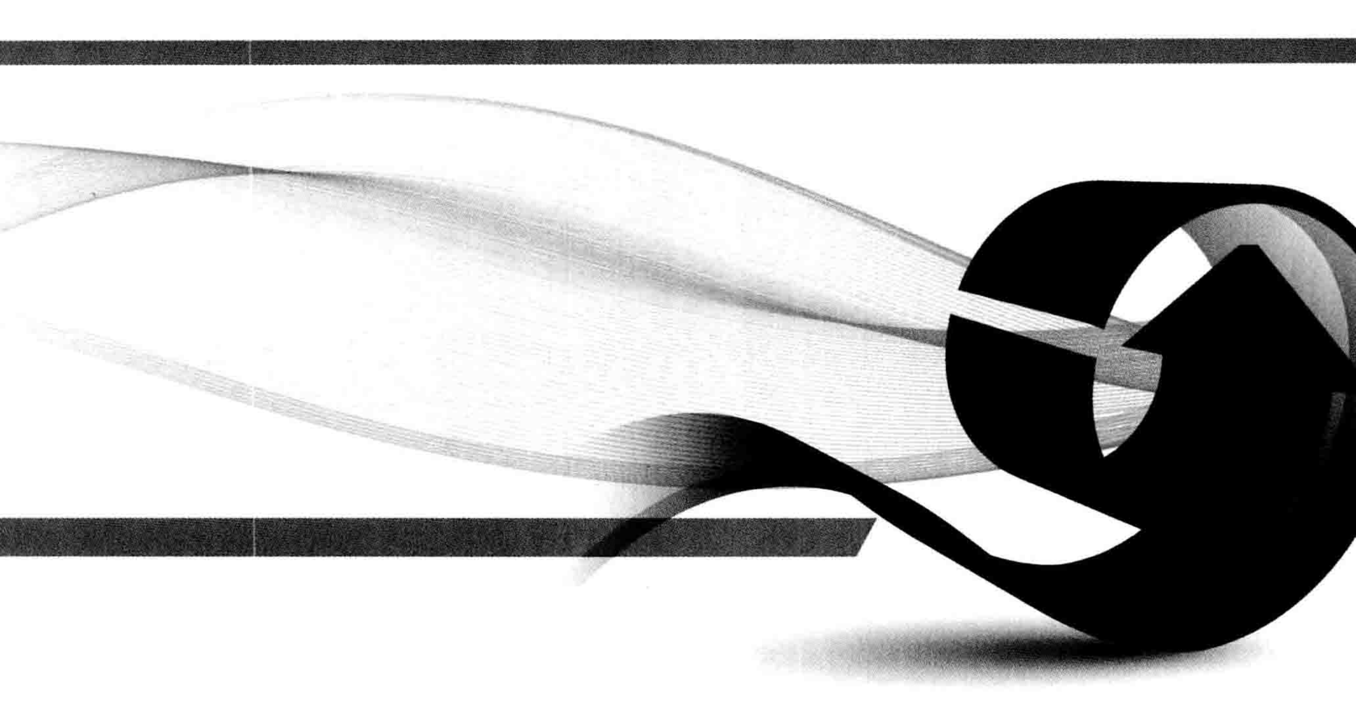
9.1 接口备份基础

9.2 接口备份配置与管理

9.3 接口备份配置示例

9.4 双机热备份基础

9.5 通过VRRP实现流量切换的双机热备份功能的配置与管理



接口备份与双机热备份是华为AR G3系列路由器的另两个用于提高网络可靠性的解决方案。它们与上一章介绍的VRRP主备备份技术有些类似，都可以实现主备切换和负载分担，但它们之间也有本质区别。

VRRP主备备份技术适用于多个网关设备的主备切换和负载分担，而接口备份则是同一设备上的多个接口之间的主备切换和负载分担；双机热备份与VRRP主备备份技术的联系更加紧密些，因为它可以与VRRP备份组进行绑定，通过HSB备份组与VRRP备份组状态联动实现主备之间的流量切换，但双机热备份技术不限定应用于网关位置，可以是任意位置，而且除了可以实现主备切换外，还可以实现双机业务信息（如防火墙功能、DHCP、NAC和WLAN等业务信息）的批量或实时备份。

本章将具体、全面地介绍AR G3系列路由器中的接口备份和双机热备份功能的配置与管理方法。总体来说，这两种可靠性功能的配置与管理都比较简单，本章有大量典型的示例，可使读者朋友更加容易理解这两种功能的配置思路和方法。

9.1 接口备份基础

重要的业务数据传输需要有高可靠性的传输线路，如果数据业务由一条链路来传输，就容易出现“单点故障”导致业务中断。此时，可以采用接口备份技术来解决这一问题。接口备份一般用于存在主备上行链路的场景，是指同一设备上的接口之间形成冗余、备份关系。当主接口出现故障或者带宽不足时，可以将流量快速地切换到备份接口，提高数据业务的可靠性。

9.1.1 接口备份概述

与上章介绍的 VRRP 技术一样，接口备份也是保证业务通畅的一个重要手段。它可实现在路由器上某个接口出现故障或者带宽不足时，通过配置接口备份，快速平滑地将该接口上的业务切换到其他正常接口。但与 VRRP 技术不一样的是，接口备份技术不是双设备间的冗余、备份，而是同一设备上的多接口间的冗余、备份，所以接口备份技术可以应用在网络中各位置设备上，而不像 VRRP 技术仅能应用于网关设备上。

接口备份中涉及以下三个基本概念。

1. 主接口

主接口为当前承担业务传输的设备接口。

2. 备份接口

备份接口是为主接口提供备份功能的接口。

3. 备份接口优先级

在配置备份接口时可配置其优先级，优先级数值越大表示其优先级越高。在主备接口备份方式下，主接口 Down 后优先级较高的备份接口将优先被启用。在负载分担接口备份方式下，主接口流量超过阈值时，优先级较高的备份接口将优先被启用；主接口流量低于阈值时，优先级较低的备份接口将首先被关闭。

在 AR G3 系列路由器中，可以作为主接口和备份接口的接口包括：三层以太网接口及其子接口、Dialer 接口、ATM 接口、ISDN BRI 接口、3G 接口、PON 接口、Async 接口、MP-group 接口、MFR 及其子接口和 Serial 接口及其子接口。这些接口均为 WAN 接口，但主、备接口可以是不同的接口类型。

说明 AR150/150-S/200/200-S 系列路由器的主接口和备份接口皆不支持 ISDN BRI 接口、PON 接口及 Async 接口。

一台设备上最多允许同时存在 10 个主接口。一个主接口最多可以有 3 个备份接口，**一个备份接口同时只能为一个主接口提供备份。**当主接口出现故障时，多个备份接口根据优先级来决定接替主接口工作的顺序。当优先级相同时，优先启动最先配置的备份接口。

主接口不能配置为其他接口的备份接口，备份接口也不能配置成其他接口的主接口。

9.1.2 接口备份主要特性

在 AR G3 系列路由器中，接口备份特性主要体现在三方面：主备接口备份功能、负

载分担接口备份功能和主备接口备份与其他功能联动。其中主备接口备份的联动功能方面又包括与 BFD、NQA 和路由的联动功能。下面分别予以介绍。

1. 主备接口备份功能

如图 9-1 所示，在 RouterA 与 RouterB 间有三条直接相连的链路（**主要应用于局域网相连中**），通过主备接口备份基本功能可配置 Interface2 接口作为主接口，Interface1 接口和 Interface3 接口作为备份接口（类似于链路聚合中的链路备份能）。这样，当 Interface2 对应的主链路故障时，可以将业务切换到备份接口，从而提高了业务传输的可靠性。

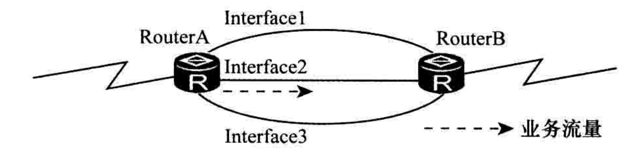


图 9-1　主备接口备份功能应用示例 1

在本示例中，在主备接口备份方式下，任意时间只有一个接口进行业务传输。

① 当主接口 Interface2 正常工作时，Interface1、Interface3 处于备份状态（不传输业务数据），通过主接口 Interface2 进行业务传输。

② 路由器跟踪各接口状态，当主接口 Interface2 因故障无法进行业务传输时，启动优先级最高的备份接口进行业务传输。

③ 当原先故障的主接口恢复正常时，业务传输会重新切换回主接口 Interface2。

图 9-2 所示为主备接口备份功能在局域网与广域网（主要是 Internet）间相连的一种应用。某企业的出口网关 RouterA 通过 ADSL 接口 ATM3/0/0 接入 Internet，为了防止出现因 ADSL 接口故障导致企业用户无法连接到 Internet 的情况，该企业同时配置了通过 3G 接口接入 Internet 的备份链路。当 ADSL 主接口故障时，启用备份链路，提高了网络可靠性。

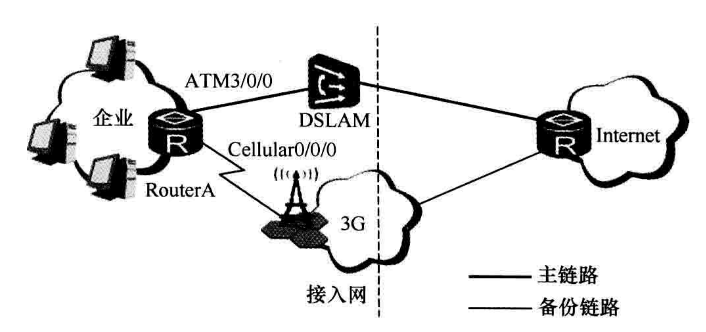


图 9-2　主备接口备份功能应用示例 2

说明 **主备接口备份功能只能检测出直连链路的故障**，当主接口上行非直连链路故障时，由于无法检测，系统不会进行主备接口切换，将会导致业务传输中断。为了检测整条链

路的状态，可使用本节后面将要介绍的主备接口备份与 NQA、BFD 或路由联动功能。这一点与上章介绍的 VRRP 技术是类似的。

2. 负载分担接口备份

与前面介绍的主备接口基本功能的两种应用环境一样，负载分担接口备份也有对应的两种应用环境。在如图 9-1 所示的应用中，可以在三条直连链路间配置负载分担功能（类似于链路聚合中的负载分担功能），如配置 Interface2 接口作为主接口，Interface1 接口和 Interface3 接口作为备份接口。当 Interface2 的带宽不足时，启用备份接口来分担流量，如图 9-3 所示。

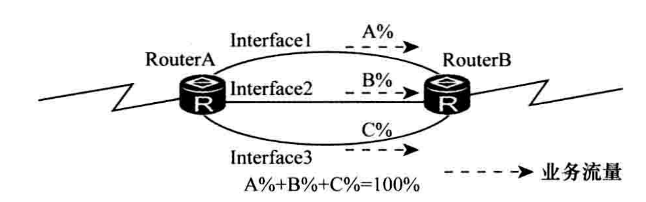


图 9-3 负载分担接口备份应用示例

在本示例中，在负载分担接口备份方式下，系统会定时检测主接口 Interface2 流量是否超过设置的门限阈值。

① 当主接口 Interface2 的数据流量超过负载分担门限的上限阈值时，优先级最高的可用备份接口将被启用，与主接口 Interface2 一起传输业务，进行负载分担。

② 如果负载分担后流量还是超过上限阈值，优先级次高的另一个可用的备份接口将被启用，在这三个接口间进行负载分担，依此类推，直至启用了所有的备份接口。

③ 在负载分担过程中，如果流量低于设定的下限阈值，优先级最低的在用备份接口将被关闭。依此类推，直至仅有主接口 Interface2 承担业务流量。

同理，也可以在图 9-2 所示的主备接口备份基本功能应用示例中为两条 WAN 线路配置负载分担功能，具体示例图略。

说明 主备接口间最终是采用主备接口备份基本功能，还是负载分担接口备份功能，是根据用户是否配置了负载分担的百分比门限决定的。一旦配置了百分比门限，则采用负载分担接口备份，否则采用主备接口备份。

主备接口备份基本功能和负载分担接口备份这两种工作方式不会同时生效：在主备接口备份基本功能方式下，即使主接口流量超出其负荷，也不会启用备份接口对流量进行分流；而在负载分担接口备份下，当主接口因故障而无法传输数据时，会启用优先级最高的一个备份接口接替原来主接口的工作，**但是负载分担功能不会生效**，因为此时生效的是主备接口备份功能。

3. 主备接口备份与 BFD/NQA/路由联动

配置主备接口备份基本功能时，如果主接口的上行非直连链路出现故障，是无法感知的，将导致业务中断，这时就可以通过与 BFD、NQA 或者路由联动来实现切换，因为通过上节的学习，我们已知道 BDF、NQA 和路由功能都可以实现对上行接口非直连

链路的故障检测。有关 BFD 和 NQA 的详细介绍请参见本书第 7 章。

BFD 提供了通用的、标准化的、介质无关、协议无关的快速故障检测机制，可以对两台路由器间双向转发路径的故障实现毫秒级的检测。通过配置接口备份与 BFD 联动功能可以对主链路的连通状态进行快速检测，实现主链路故障时主备链路的快速切换，提高了业务传输的可靠性。

NQA 是一种实时的网络性能探测和统计技术，通过对响应时间、网络抖动、丢包率等网络信息进行统计，可以清晰地反映出网络的畅通情况。通过配置主备接口备份功能与 NQA 联动功能也可以对主链路的连通状态进行实时检测，实现主链路故障时主备链路的快速切换，提高了业务传输的可靠性。

路由状态可以反映出一条链路的连通状况，当链路故障时，路由会撤销或状态变为非激活。通过配置接口备份与路由联动功能也可以对主链路的连通状态进行检测，实现主链路发生故障时主备链路的快速切换，提高了业务传输的可靠性。

如图 9-4 所示，公司总部的出口网关 RouterA 通过接口 GE1/0/0 接入 Internet 作为业务传输的主链路与公司分部进行通信，ADSL 接口 ATM0/0/0 接入 Internet 作为备份链路。通过与 BFD 联动时，可在 RouterA 和 RouterB 上配置 BFD 会话，并在备份接口 ATM0/0/0 上配置接口备份与 BFD 联动。这样可实现在 RouterD 到 RouterB 间的链路发生故障时，BFD 会话快速检测出故障并通知 RouterA 启用备份接口 ATM0/0/0，由备份链路临时承担业务传输。

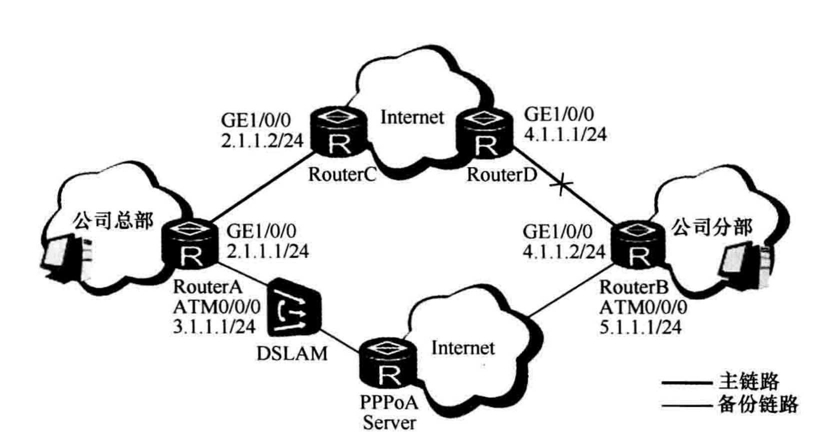


图 9-4　主备接口备份与 BFD/NQA/路由联动应用示例

如果要采用与 NQA 联动的方法，可在 RouterA 上配置 NQA 测试例，并在备份接口 ATM0/0/0 上配置接口备份与 NQA 联动。这样也可实现在 RouterD 到 RouterB 之间链路发生故障时，NQA 测试例可以检测出故障并通知 RouterA 启用备份接口 ATM0/0/0，由备份链路临时承担业务传输。

如果要使用与路由联动的功能，则可在备份接口 ATM0/0/0 上配置接口备份与路由联动，检测主链路的路由状态。这样也可实现在 RouterD 到 RouterB 之间链路发生故障时，路由模块感知主链路路由撤销，通知 RouterA 启用备份接口 ATM0/0/0，由备份链路临时承担业务传输。

9.2 接口备份配置与管理

在上节已介绍 AR G3 系列路由器的接口备份功能支持主备接口备份基本功能、负载分担接口备份功能和主备接口备份与 BFD/NQA/路由联动功能这三种特性。但要注意的是，**这三种特性是彼此之间平等的，各自需要独立配置**，而不像上章介绍的 VRRP 配置中 VRRP 基本功能是其他特性配置的前提。

9.2.1 配置主备接口备份基本功能

配置主备接口备份基本功能，可以使主接口及所在直连链路因故障而无法进行业务传输时，启用备份接口，以提高业务传输的可靠性。配置好主备接口备份基本功能后，当主接口 Down 时，这些备份接口会根据优先级的高低决定启用顺序，优先级最高的接口优先被启用；如果各备份接口优先级相同，则会优先选择先配置的备份接口。

主备接口备份基本功能的配置很简单，主要就是两个方面的配置：一是在主接口视图下配置各备份接口及优先级，二是配置主备接口的切换延时，具体配置步骤如表 9-1 所示。在配置主备接口备份基本功能前，需配置主链路和备份链路的路由协议，保证各自的网络层连通。

说明 可以作为主接口和备份接口的接口包括三层以太网接口及其子接口、Dialer 接口、ATM 接口、ISDN BRI 接口、3G 接口、PON 接口、Async 接口、MP-group 接口、MFR 及其子接口和 Serial 接口及其子接口，**但必须是 WAN 侧接口，不能是 LAN 侧接口。**

表 9-1 主备接口备份基本功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入主接口，进入接口视图
3	**standby interface** *interface-type interface-number* [*priority*] 例如：[Huawei-GigabitEthernet1/0/0] **standby interface** gigabitethernet 2/0/0 20	配置主接口的备份接口并配置其优先级。命令中的参数说明如下 ● *interface-type interface-number*：指定要作为主接口的备份接口（必须是与主接口在同一设备上的 WAN 侧接口） ● *priority*：可选参数，指定所配置的备份接口所在的优先级，取值范围为 0～255 的整数，**值越大，优先级越高**，缺省值为 0 【注意】**一台设备上最多允许同时存在 10 个主接口，一个主接口最多可以配置 3 个备份接口**。如果需要配置多个备份接口，则需要重复配置本命令。**但一个备份接口同时只能为一个主接口提供备份**；主接口不能配置为其他接口的备份接口，备份接口也不能配置成其他接口的主接口 缺省情况下，系统中无任何备份接口，可用 **undo standby interface** *interface-type interface-number* 命令删除指定主接口的备份接口

（续表）

步骤	命令	说明
4	**standby timer delay** *enable-delay disable-delay* 例如：[Huawei-GigabitEthernet1/0/0] **standby timer delay** 10 10	（可选）配置主备接口切换延时。命令中的参数说明如下 ● *enable-delay*：指定主接口切换到备份接口的延时，取值范围为 0～65 535 的整数秒。缺省延时为 5 s ● *disable-delay*：指定备份接口切换到主接口的延时，取值范围为 0～65 535 的整数秒。缺省延时为 5 s 【说明】当路由器升级或者主备倒换时，容易导致接口状态不稳定，使主备接口频繁切换，可能引起网络振荡。为避免该情况，可通过本命令设置主备接口切换延时。即当主接口状态由 Up 转为 Down 掉后，系统并不立即切换到备份接口，而是等待一个预先设置好的延时。如果超过这个延时后，主接口的状态仍为 Down 状态，切换到备份接口；如果在延时时间段中，主接口状态恢复正常，则不进行切换 对于传输数据要求不高的网络，可以将切换延时时间配置较大值，防止网络振荡的现象；而对于传输数据要求较高的网络，建议将切换时间配置较小值，防止数据流量的丢失 缺省情况下，主备接口切换延时为 5 s，可用 undo standby timer delay 命令恢复主备接口切换延时为缺省值

9.2.2　配置负载分担接口备份

负载分担接口备份与上节介绍的主备接口备份基本功能相比，最大的区别就是可以在主接口带宽不足时，使各备份接口参与到主接口的数据业务传输，从而提高数据传输的可靠性。在配置方法上，与上节介绍的主备接口备份基本功能相比，主要区别有两个方面。

① 在负载分担接口备份功能中不需要配置主备接口切换延时，因为主备接口备份和负载分担接口备份是两种不能共存的方式，只能工作在一种方式下。

② 在负载分担接口备份功能中多了负载分担的百分比门限及相关参数配置。

具体配置步骤如表 9-2 所示。但在配置负载分担接口备份之前，也需配置主链路和备份链路各自的路由协议，以保证各自链路在网络层连通。**如果采用动态路由协议，建议主接口和备份接口到目的网段的路由采用等价路由配置。**

表 9-2　　负载分担接口备份的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入主接口，进入接口视图
3	**standby interface** *interface-type interface-number* [*priority*] 例如：[Huawei-GigabitEthernet1/0/0] **standby interface** gigabitethernet 2/0/0 20	配置主接口的备份接口并配置其优先级 【说明】如果多个备份接口配置不同的优先级，优先级数值越大表示将被启用或关闭的优先级越高，即在主接口带宽不足时，优先级高的备份接口将优先启用进行负载分担；当流量小于主接口带宽时，优先级最低的将优先退出负载分担进程；如果多个备份接口的优先级相同，将根据其配置的先后

（续表）

步骤	命令	说明
3	**standby interface** *interface-type interface-number* [*priority*] 例如：[Huawei-GigabitEthernet1/0/0] **standby interface** gigabitethernet 2/0/0 20	顺序来决定备份接口的启用或关闭，即在主接口带宽不足时，先配置的备份接口将被优先启用参与负载分担；而当流量小于主接口带宽时，后配置的备份接口将被优先退出负载分担进程 其他说明参见上节表 9-1 中的第 3 步
4	**standby threshold** *enable-threshold disable-threshold* 例如：[Huawei-GigabitEthernet1/0/0] **standby threshold** 80 20	配置负载分担门限的上限和下限阈值。命令中的参数说明如下。 ● *enable-threshold*：指定负载分担门限上限百分比，取值范围为 1～99 的整数。 ● *disable-threshold*：指定负载分担门限下限百分比，取值范围为 1～99 的整数 【注意】*enable-threshold* 参数的取值必须大于 *disable-threshol d* 参数的取值 在缺省情况下，系统没有使能接口备份的负载分担功能。**一旦通过本命令配置了百分比门限，则表示采用负载分担方式，否则采用主备备份方式。** 配置负载分担功能后，**如果主接口发生故障，系统将转换为主备接口备份模式**。具体又分以下两种情况。 ● 如果主接口故障时未启用备份接口（就是当前没有备份接口参与负载分担），则启用优先级最高的备份接口进行业务传输，优先级相同时，启用先配置的备份接口 ● 如果主接口故障时已启用备份接口（就是当前已有备份接口参与负载分担），则保留优先级最高的备份接口进行业务传输，优先级相同时，保留最先配置的备份接口 缺省情况下，没有配置负载分担门限，可用 **undo standby threshold** 命令恢复负载分担门限的上限和下限阈值的缺省值，此时**如果已经有备份接口被启用，将关闭所有的备份接口，只保留主接口**
5	**standby bandwidth** *size* 例如：[Huawei-GigabitEthernet1/0/0] **standby bandwidth 10000**	（可选）配置负载分担方式下主接口的最大可用带宽，取值范围为 0～4 000 000 bit/s，当然不能超出具体主接口的实际物理带宽 缺省情况下，主接口的最大可用带宽为主接口实际物理带宽，可用 **undo standby bandwidth** 命令恢复负载分担方式下主接口的最大可用带宽为缺省值
6	**standby timer flow-check** *time* 例如：[Huawei-GigabitEthernet1/0/0] **standby timer flow-check** 60	（可选）配置检测主接口流量的时间间隔，取值范围为（10～600）的整数秒 缺省情况下，检测主接口流量的时间间隔为 10 s，可用 **undo standby timer flow-check** 命令恢复流量检测时间间隔为缺省值

9.2.3 配置主备接口备份联动功能

配置主备接口备份联动功能，可在主链路因发生故障而无法进行业务传输时，启用备份接口，提高业务传输的可靠性，包括以下三种联动方式。

① 配置主备接口备份与 BFD 联动功能。

② 配置主备接口备份与 NQA 联动功能。

③ 配置主备接口备份与路由联动功能。

下面分别对以上三种联动功能的配置方法进行具体介绍。

1. 配置主备接口备份与 BFD 联动功能

BFD 提供了通用的、标准化的、介质无关、协议无关的快速故障检测机制，可以为各上层协议如路由协议、MPLS 等统一地快速检测两台路由器间双向转发路径的故障。通过配置接口备份与 BFD 联动功能可以对主链路的连通状态进行快速检测，实现主链路故障时主备链路的快速切换，以保证业务正常传输。

说明　如果配置接口备份的主链路和备份链路采用静态路由，由于静态路由自身没有收敛机制，当主链路出现故障时，会因为路由不能及时切换而造成数据流量丢失。因此，为了保证数据流能正常切换，可以配置备份链路路由的优先级比主链路的优先级高；或者配置静态路由与 BFD 联动，当 BFD 会话检测到主链路不可达时，删除路由表中主链路对应的静态路由。有关静态路由与 BFD 联动的具体配置方法将在本书第 10 章进行介绍。

接口备份与 BFD 联动功能的配置步骤如表 9-3 所示，但在配置之前，需按照前面的说明配置主链路和备份链路各自的路由协议，保证网络层连通。且接口备份与 BFD 联动功能仅支持联动静态和静态自协商类型的 BFD 会话。**有关这两种 BFD 会话的配置方法请参见本书第 7 章。**

表 9-3　主备接口备份与 BFD 联动功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] } [**preference** *preference* | **tag** *tag*] * [**track bfd-session** *cfg-name*] [**description** *text*] 例如：[Huawei]**ip route-static** 4.1.1.0 255.255.255.0 2.1.1.2 **preference** 80	（可选）为主链路的 IPv4 静态路由绑定 BFD 会话，或者配置主、备链路的路由优先级（**要求分别配置主备链路的静态路由，且备份链路静态路由优先级高于主链路静态路由的优先级，但要注意：路由优先级是值越大，优先级越低**）。命令中的参数说明如下 ● *ip-address*：指定静态路由的目的 IP 地址 ● *mask* | *mask-length*：指定静态路由的目的 IP 地址所对应的子网掩码（选择 *mask* 参数时）或子网掩码长度（选择 *mask-length* 参数时）。如果目的 IP 地址和掩码都为 0.0.0.0，配置的路由为缺省路由。如果检查路由表时没有找到相关路由，则使用缺省路由进行报文转发 ● *nexthop-address*：二选一参数，指定静态路由的下一跳 IP 地址 ● *interface-type interface-number* [*nexthop-address*]：二选一参数，指定静态路由的出接口，或同时指定静态路由的下一跳 IP 地址 ● **preference** *preference*：可多选参数，指定静态路由的优先级，取值范围是 1～255。**值越大，优先级越低**。如果不配置此可选参数，则采用默认优先级 60 ● **tag** *tag*：可多选参数，指定静态路由的 tag 属性值。配置不同的 tag 属性值，可对静态路由进行分类，以实现不同的路由管理策略。例如，其他协议引入静态路由时，可通过路由策略引入具有特定 tag 属性值的路由

（续表）

步骤	命令	说明
2	**ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] } [**preference** *preference* | **tag** *tag*] * [**track bfd-session** *cfg-name*] [**description** *text*] 例如：[Huawei]**ip route-static** 4.1.1.0 255.255.255.0 2.1.1.2 **preference** 80	• **bfd-session** *cfg-name*：可选参数，指定与静态路由进行绑定的静态 BFD 会话的名称，1～15 个字符，不支持空格 • **description** *text*：可选参数，指定静态路由的描述信息，1～35 个字符，支持空格 【说明】**当主链路和备份链路采用静态路由时，才需要执行本步，而当主链路和备份链路采用动态路由时，不需要执行本步** 配置静态路由时，可根据实际需要指定出接口或下一跳 IP 地址。对于点到点接口，只需指定出接口；对于 NBMA（Non Broadcast Multiple Access，非广播多路访问）接口，只需配置下一跳；对于广播类型接口，必须指定下一跳 IP 地址 在某些情况下，如链路层被 PPP 封装，即使不知道对端地址，也可以在路由器配置时指定出接口。这样，即使对端地址发生了改变也无需改变该路由器的配置 缺省情况下，没有为主链路的 IPv4 静态路由绑定 BFD 会话或者没有配置主备链路的路由优先级，可用 **undo ip route-static** *ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number [nexthop-address]] [preference preference* | **tag***tag*] * **track bfd-session** 命令为主链路的 IPv4 静态路由绑定的 BFD 会话，或者删除配置的主备链路的路由优先级
3	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入**备份接口**，进入接口视图
4	**standby track bfd-session session-name** *session-name* 例如：[Huawei-GigabitEthernet1/0/0] **standby track bfd-session session-name** test	使能接口备份与 BFD 联动功能。参数 *session-name* 用来指定与接口备份功能联动的 BFD 会话的名称，1～15 个字符，不支持空格，**不区分大小写** 【注意】一个备份接口只能联动一个 BFD 会话，而同一个 BFD 会话可以为多个备份接口配置联动功能 缺省情况下，未使能接口备份与 BFD 联动功能，可用 **undo standby track bfd-session session-name** *session-name* 命令去使能对应备份接口的接口备份与指定 BFD 会话的联动功能
如果有多个备份接口，则要分别进行第 3～4 步的配置		

2. 配置主备接口备份与 NQA 联动功能

NQA 是一种实时的网络性能探测和统计技术，可以对响应时间、网络抖动、丢包率等网络信息进行统计。当 NQA 检测到主链路状态良好时，由主链路承担业务传输；当 NQA 检测到主链路不可达或链路质量较差时，通知设备启用备份接口，由备份链路临时承担业务传输；当 NQA 检测到原先故障的主链路恢复正常时，业务会重新切换到主链路。

说明 与前面介绍的接口备份与 BFD 会话联动一样，在接口备份与 NQA 联动的配置中，如果配置接口备份的主链路和备份链路采用静态路由，由于静态路由自身没有收敛机制，当主链路出现故障时，会因为路由不能及时切换而造成数据流丢失。因此，为了保证数

据流能正常切换，可以配置备份链路的路由优先级比主链路的优先级高；或者配置静态路由与 NQA 联动，当 NQA 测试例检测到主链路不可达时，删除路由表中主链路对应的静态路由。

接口备份与 NQA 联动功能的配置步骤如表 9-4 所示，整体上与前面介绍的与 BFD 联动的配置差不多。但在配置之前，需按照前面的说明配置主链路和备份链路各自的路由协议，保证网络层连通。但接口备份与 NQA 联动功能仅支持联动 ICMP 类型的 NQA 测试例。**有关这两种 NQA ICMP 测试例的配置方法请参见本书第 7 章。**

表 9-4　　主备接口备份与 NQA 联动功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] } [**preference** *preference* | **tag** *tag*] * [**track nqa** *admin-name test-name*] [**description** *text*] 例如：[Huawei]**ip route-static** 4.1.1.0 255.255.255.0 2.1.1.2 **preference** 80	（可选）为主链路的 IPv4 静态路由绑定 NQA 会话，或者配置主、备链路的路由优先级（**要求分别配置主备链路的静态路由，且备份链路静态路由优先级高于主链路静态路由的优先级，但要注意：路由优先级是值越大，优先级越低**）。命令中的 **track nqa** *admin-name test-name* 可选参数分别用来创建要与主备接口备份联动的 NQA 测试例的管理员账户名称，指定 NQA 测试例名称，均为 1～32 个字符，不支持空格，区分大小写。命令中的其他参数指说明参见表 9-3 中的第 3 步 【说明】**当主链路和备份链路采用静态路由时，才需要执行本步，而当主链路和备份链路采用动态路由时，不需要执行本步** 缺省情况下，没有为主链路的 IPv4 静态路由绑定 NQA 会话或者没有配置主备链路的路由优先级，可用 **undo ip route-static** *ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag***tag*] * [**track nqa**]命令为主链路的 IPv4 静态路由绑定 NQA 会话，或者删除配置的主备链路的路由优先级
3	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入**备份接口**，进入接口视图
4	**standby track nqa** *admin-name test-name* 例如：[Huawei-GigabitEthernet1/0/0]**standby track nqa** user test	使能接口备份与 NQA 联动功能。参数 *admin-name test-name* 分别用来指定与接口备份功能联动的 NQA 测试例的管理者名和测试例名，均为 1～32 个字符，不支持空格，**区分大小写** 【注意】一个备份接口只能联动一个 NQA 测试例，而同一个 NQA 测试例可以为多个备份接口配置联动功能 缺省情况下，未使能接口备份与 NQA 联动功能，可用 **undo standby track nqa** *admin-name test-name* 命令去使能对应备份接口的接口备份与指定 NQA 会话的联动功能
如果有多个备份接口，则要分别进行第 3～4 步的配置		

3. 配置主备接口备份与路由联动功能

通过在设备的备份接口上配置接口备份与路由联动，即可实现对主链路路由状态的检测和主备链路的切换。接口备份模块监控设备上行链路的路由条目，如果路由撤销或

变为非活跃状态，则启用备份接口，由备份链路来临时承担业务传输；当路由状态恢复正常时，业务会重新切换到主链路。但接口备份与路由联动功能仅支持联动动态路由。

配置接口备份与路由联动功能的方法很简单，仅需在备份接口视图下使用 **standby track ip route** *ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*] 命令配置接口备份和路由联动功能。但在配置接口备份与路由联动功能之前，需配置主链路和备份链路各自的路由协议，保证网络层连通。命令中的参数说明如下。

① *ip-address*：指定接口备份功能联动的动态路由的目的 IP 地址，是一个主机 IP 地址。

② *mask-address* | *mask-length*：指定以上动态路由的目的 IP 地址所对应的子网掩码（选择 *mask* 参数时）或子网掩码长度（选择 *mask-length* 参数时）。

③ **vpn-instance** *vpn-instance-name*：可选参数，指定要应用接口备份与路由联动功能的 VPN 实例的名称，1～31 字符，不支持空格，**区分大小写。**

缺省情况下，未使能接口备份与路由联动功能，可用 **standby track ip route** 命令使能接口备份与路由联动功能。

【示例】指定接口 GE1/0/0 作为备份接口，并在 GE1/0/0 上配置接口备份与到达 10.1.1.2/24 的动态路由进行联动。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] standby track ip route 10.1.1.2 24
```

4. 接口备份管理

接口备份管理包括上节介绍的主备接口备份基本功能和本节介绍的接口备份与各种其他技术联动功能，都可以使用 **display standby state** 任意视图命令查看各接口备份的配置和状态信息，验证配置结果。

9.3 接口备份配置示例

本节将通过几个在当前实际工作中常见的具体示例巩固上节介绍的各种接口备份功能的配置方法。

9.3.1 以太链路+以太链路的主备接口备份配置示例

本示例的基本拓扑结构如图 9-5 所示，是一个典型的多以太网链路主备接口备份应用。RouterA 通过 3 个接口与 RouterB 直接直连，正常情况下，HostA 通过 RouterA 的 GE2/0/0 接口与 HostB 进行数据传输。为了提高 HostA 与 HostB 间数据传输的可靠性，用户希望当 GE2/0/0 接口出现故障时，能够优先将流量切换到 GE1/0/0 接口。

1. 基本配置思路分析

根据 9.2.1 小节介绍的主备接口备份基本功能的配置方法，结合本示例的具体要求，可以得出本示例的基本配置思路如下。

① 配置各接口 IP 地址及 HostA 与 HostB 三条链路各自的静态路由，确保每条链路的网络层互通。

② 在 RouterA 上配置 GE2/0/0 为主接口，GE1/0/0 和 GE3/0/0 为 GE2/0/0 的备份接口，且 GE1/0/0 的优先级较高，实现主接口故障时，GE1/0/0 优先提供备份服务。

③ 配置主接口与备份接口相互切换的延时，避免主备接口频繁切换而导致网络振荡。

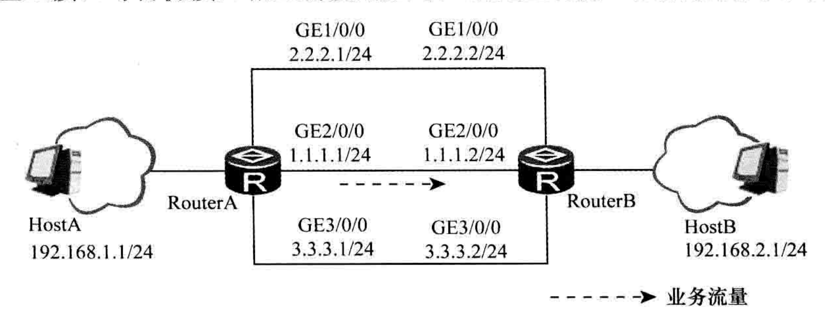


图 9-5　以太链路+以太链路主备接口备份配置示例拓扑结构

2. 具体配置步骤

① 配置各接口 IP 地址及 HostA 与 HostB 之间的静态路由。

下面先配置各接口的 IP 地址，仅以 RouterA 为例，RouterB 的配置类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 1.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 2.2.2.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 3.3.3.1 255.255.255.0
[RouterA-GigabitEthernet3/0/0] quit
```

然后配置三条链路到达对端网络主机的各自往返静态路由。注意：静态路由具有单向性，需要配置好双向静态路由，具体将在本书第 10 章介绍。

下面是在 RouterA 上配置去往 HostB 所在网段的三条静态路由。

```
[RouterA] ip route-static 192.168.2.0 24 2.2.2.2
[RouterA] ip route-static 192.168.2.0 24 1.1.1.2
[RouterA] ip route-static 192.168.2.0 24 3.3.3.2
```

下面是在 RouterB 上配置去往 HostA 所在网段的三条静态路由。

```
[RouterB] ip route-static 192.168.1.0 24 2.2.2.1
[RouterB] ip route-static 192.168.1.0 24 1.1.1.1
[RouterB] ip route-static 192.168.1.0 24 3.3.3.1
```

② 在 RouterA 上配置 GE2/0/0 为主接口，GE1/0/0 和 GE3/0/0 为备份接口，且 GE1/0/0 和 GE3/0/0 的优先级分别为 30 和 20，即 GE1/0/0 优先级更高。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby interface gigabitethernet 1/0/0 30
[RouterA-GigabitEthernet2/0/0] standby interface gigabitethernet 3/0/0 20
[RouterA-GigabitEthernet2/0/0] quit
```

③ 在 RouterA 上配置主备接口切换的延时均为 10 s。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby timer delay 10 10
[RouterA-GigabitEthernet2/0/0] quit
```

配置好后，在 RouterA 上执行 **display standby state** 命令查看主备接口的状态信息，可以看到主接口 GigabitEthernet2/0/0 的状态是 UP，备份接口 GigabitEthernet1/0/0 和 GigabitEthernet3/0/0 的状态是 STANDBY。

```
<RouterA> display standby state
Interface                          Interfacestate Backupstate Backupflag Pri Loadstate
GigabitEthernet2/0/0                        UP          MUP          MU
GigabitEthernet1/0/0                   STANDBY     STANDBY           BU   30
GigabitEthernet3/0/0                   STANDBY     STANDBY           BU   20
Backup-flag meaning:
M---MAIN  B---BACKUP     V---MOVED    U---USED
D---LOAD  P---PULLED


------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name                  Bfd-State   BackupInterface              State

------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask       Route-State   BackupInterface               State

------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                        BackupInterface               State
```

在 RouterA 主接口 GE2/0/0 上执行 **shutdown** 命令，模拟链路故障，然后执行 **display standby state** 命令，可以看到主接口 GigabitEthernet2/0/0 状态为 DOWN，备份接口 GigabitEthernet1/0/0 的状态为 UP，表示备份接口已经启用。

```
<RouterA> display standby state
Interface                          Interfacestate Backupstate Backupflag Pri Loadstate
GigabitEthernet2/0/0                      DOWN        MDOWN              MU
GigabitEthernet1/0/0                        UP          UP          BU   30
GigabitEthernet3/0/0                   STANDBY     STANDBY           BU   20
Backup-flag meaning:
M---MAIN  B---BACKUP     V---MOVED    U---USED
D---LOAD  P---PULLED


------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name                  Bfd-State   BackupInterface              State

------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask       Route-State   BackupInterface               State

------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                        BackupInterface               State
```

9.3.2 以太链路+以太链路的负载分担接口备份配置示例

本示例的基本拓扑结构如上节的图 9-5 所示在本示例中，为了提高 HostA 与 HostB

间数据传输的可靠性，用户希望当 GE2/0/0 接口上流量达到其最大可用带宽的 80%时，优先启动 GE1/0/0 接口进行负载分担，当 GE2/0/0 接口上流量低于此带宽的 20%时，关闭优先级较低的接口。

1. 基本配置思路分析

本示例是典型的多以太网链路负载分担应用，可采用如下的基本配置思路在接口上配置负载分担接口备份。

① 配置各接口的 IP 地址及 HostA 与 HostB 之间的静态路由，实现网络层互通（直接参见上节的第 1 步）。

② 在 RouterA 上配置 GE2/0/0 为主接口，GE1/0/0 和 GE3/0/0 为 GE2/0/0 的备份接口，且 GE1/0/0 的优先级较高。这样就实现了主接口流量过高时，优先启用 GE1/0/0 进行负载分担的目的。

③ 配置主接口最大可用带宽及负载分担的百分比门限，确定启用备份接口的条件。

2. 具体配置步骤

① 配置各接口 IP 地址及 HostA 与 HostB 之间静态路由的步骤略，可直接参见上节的第（1）步配置。

② 在 RouterA 上配置主备接口及备份接口优先级，即配置 GE2/0/0 为主接口，GE1/0/0 和 GE3/0/0 为备份接口，且 GE1/0/0 和 GE3/0/0 的优先级分别为 30 和 20。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby interface gigabitethernet 1/0/0 30
[RouterA-GigabitEthernet2/0/0] standby interface gigabitethernet 3/0/0 20
[RouterA-GigabitEthernet2/0/0] quit
```

③ 在 RouterA 上配置主接口的最大可用带宽为 10 000 kbit/s。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby bandwidth 10000
[RouterA-GigabitEthernet2/0/0] quit
```

④ 在 RouterA 上配置负载分担的百分比门限的上限阈值为 80%，下限阈值为 20%。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby threshold 80 20
[RouterA-GigabitEthernet2/0/0] quit
```

配置好后，在 RouterA 上执行 **display standby state** 命令查看主备接口的状态信息，可以看到，“Loadstate”字段显示为 TO-HYPNOTIZE，表明接口处于负载分担方式，且主接口 GigabitEthernet2/0/0 的状态是 UP，备份接口 GigabitEthernet1/0/0 和 GigabitEthernet3/0/0 的状态是 STANDBY，表明配置是正确、成功的。

```
<RouterA> display standby state
Interface                    Interfacestate Backupstate Backupflag Pri Loadstate
GigabitEthernet2/0/0              UP          MUP          MU        TO-HYPNOTIZE
GigabitEthernet1/0/0           STANDBY      STANDBY          BU   30
GigabitEthernet3/0/0           STANDBY      STANDBY          BU   20
Backup-flag meaning:
M---MAIN  B---BACKUP     V---MOVED     U---USED
D---LOAD  P---PULLED


---------------------------------------------------------------------------
Below is track BFD information:
```

```
Bfd-Name                Bfd-State   BackupInterface              State

------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask       Route-State   BackupInterface              State

------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                        BackupInterface              State
```

9.3.3 ADSL 链路+3G 网络的主备接口备份配置示例

本示例的基本拓扑结构如图 9-6 所示，Router 是企业的出口网关，企业将 ADSL 接口作为主链路上行接入 Internet。为了增强企业接入 Internet 的可靠性，防止主链路发生故障而导致企业用户无法正常接入 Internet，企业希望使用 3G Cellular 接口作为备份链路上行接入 Internet。

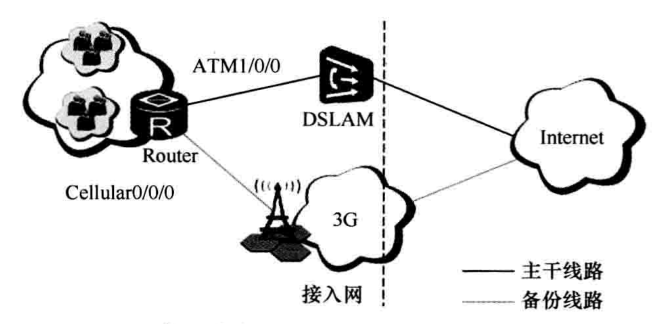


图 9-6 3G Cellular 接口作为备份链路接入 Internet 配置示例的拓扑结构

1. 基本配置思路分析

这可以算是一个双线 Internet 接入备份的应用示例，可采用如下的基本配置思路。

① 配置企业内网，指定 Router 作为企业出口网关，由 Router 为企业内网用户分配 IP 地址。

② 配置 ADSL 接口作为企业的上行主用接口。

③ 配置 3G Cellular 接口作为企业的上行备份接口。

④ 配置缺省路由，使企业内网的流量可以通过 ADSL 接口和 3G Cellular 接口上行传输到 Internet。

2. 具体配置步骤

① 配置企业内网，假设路由器连接的内网为一个 VLAN 100 网段（假设其 LAN 口为 Ethernet 2/0/0，IP 网段为 192.168.100.0/24），由路由器配置的 DHCP 服务器全局地址池为 VLAN 100 中的用户分配 IP 地址。有关 DHCP 服务器的配置参见本书第 5 章。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 100
[Router-vlan100] quit
[Router] dhcp enable
[Router] interface vlanif 100
[Router-Vlanif100] ip address 192.168.100.1 255.255.255.0
```

```
[Router-Vlanif100] dhcp select global          !---使能 VLANIF100 接口采用全局地址池的 DHCP 服务器功能
[Router-Vlanif100] quit
[Router] ip pool lan                           !---创建名为 LVAN 的全局地址池
[Router-ip-pool-lan] gateway-list 192.168.100.1   !---指定网关为 VLANIF100 接口的 IP 地址
[Router-ip-pool-lan] network 192.168.100.0 mask 24 !---指定全局地址池的 IP 地址段为 192.168.100.0/24
[Router-ip-pool-lan] quit
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type hybrid    !---配置以上接口为 Hybrid 接口类型
[Router-Ethernet2/0/0] port hybrid pvid vlan 100   !---配置以上接口的 PVID 为 VLAN 100
[Router-Ethernet2/0/0] port hybrid untagged vlan 100 !---配置以上接口以不带标签方式加入 VLAN 100 中
[Router-Ethernet2/0/0] quit
```

② 配置 ADSL 接口作为企业的上行主用接口，有关 ADSL 接口与虚拟模板接口配置请参见本书第 4 章。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.100.0 0.0.0.255   !---定义允许内部网络用户进行 IP 通信的 ACL
[Router-acl-adv-3002] quit
[Router] interface virtual-template 10          !---创建虚拟模板接口 10
[Router-Virtual-Template10] ip address ppp-negotiate !---指定虚拟模板 10 接口采用与对端协商方式获取 IP 地址
[Router-Virtual-Template10] nat outbound 3002     !---指定虚拟模板 10 允许使用 NAT 进行地址转换的内部网络用户，具体的 NAT 配置本示例没有给出，具体 NAT 配置方法参见本书第 6 章
[Router-Virtual-Template10] quit
[Router] interface atm 1/0/0
[Router-Atm1/0/0] pvc voip 1/35                 !—创建名为 voip 的 PVC，并根据 ISP 提供的 vpi/vci 值配置 PVC 的值
[Router-atm-pvc-Atm1/0/0-1/35-voip] map ppp virtual-template 10 !---创建与虚拟模板接口 10 的 PPPoA 映射
[Router-atm-pvc-Atm1/0/0-1/35-voip] quit
[Router-Atm1/0/0] standby interface Cellular 0/0/0   !---指定 3G Cellular 0/0/0 作为 ATM 1/0/0 接口的备份接口
[Router-Atm1/0/0] quit
```

说明　本示例中的 ADSL 是通过 ATM 接口与局端 DSLAM 设备连接的，即 PPPoA ADSL，而不是我们家用中常见通过以太网接口进行的 PPPoE ADSL。PPPoA 支持以下两种建立链路的类型。

- 永久在线模式：此时要使用 **map ppp virtual-template** *vt-number* 命令建立普通 PPPoA 映射。即在**专线 PPPoA ADSL 中，必须把 ATM 接口映射到虚拟模板接口上**。本示例假设是专线方式 PPPoA ADSL。
- 按需呼叫模式：此时需要使用 **map ppp virtual-template** *vt-number* 或者 **map ppp dialer** *dialer-number* 命令建立按需 PPPoA 映射。即在拨号 PPPoA ADSL 中，可以把 ATM 接口映射到虚拟模板接口或者拨号接口，通常是映射到拨号接口，因为要配置共享 DCC 拨号参数。

③ 配置 3G Cellular 接口作为企业的上行备份接口。本示例中，假设对接的 3G 网络为 WCDMA 网络，现要接入 WCDMA 的 PS 域，需要配置拨号串为“*99#”。APN 的名称需要和运营商给定的一致，现假设接入的 APN 名称为“wcdma”。配置备份接口前，请确保 3G modem 和 SIM/UIM 卡在位。

```
[Router] dialer-rule
[Router-dialer-rule] dialer-rule 1 ip permit
[Router-dialer-rule] quit
[Router] interface Cellular 0/0/0
[Router-Cellular0/0/0] profile create 1 static wcdma   !---创建索引号为 1 的 3G modem 的参数描述模板，并配置 APN 名称为 wcdma
```

```
[Router-Cellular0/0/0] link-protocol ppp              !---在 3G Cellular 0/0/0 接口上封装 PPP 协议
[Router-Cellular0/0/0] ip address ppp-negotiate       !---指定 3G Cellular 0/0/0 接口采用与对端协商方式获取 IP 地址
[Router-Cellular0/0/0] dialer enable-circular         !---在 3G Cellular 0/0/0 接口上使能轮询 DCC 功能
[Router-Cellular0/0/0] dialer-group 1                 !---创建索引号为 1 的拨号组
[Router-Cellular0/0/0] dialer timer idle 30           !---指定 3G 线路允许空闲的时间为 30 s
[Router-Cellular0/0/0] dialer number *99#             !---指定拨号串为*99#
[Router-Cellular0/0/0] nat outbound 3002
[Router-Cellular0/0/0] quit
```

④ 配置通过两条线路接入 Internet 的缺省路由。要注意的是，这里因为是通过 ATM 接口进行 ADSL 通信的，所以在配置通过 ADSL 线路的静态路由时要以其所映射的虚拟模拟接口为出接口，而不是实际的 ATM 接口，且其静态路由优先级要比通过 3G Cellular0/0/0 的静态路由优先级高（优先级值低）。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 virtual-template 10 preference 40
[Router] ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/0 preference 80
```

配置完成后，在 Router 上执行 **display standby state** 检查主备接口状态，可以看到 ATM1/0/0 接口的状态为 UP，备份接口 Cellular0/0/0 接口的状态为 STANDBY，符合要求。

```
[Router] display standby state
Interface                     Interfacestate Backupstate Backupflag Pri    Loadstate
ATM1/0/0                                    UP             MUP        MU
Cellular0/0/0                         STANDBY       STANDBY         BU      0

 Backup-flag meaning:
 M---MAIN   B---BACKUP      V---MOVED      U---USED
 D---LOAD   P---PULLED


--------------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name                  Bfd-State   BackupInterface                 State

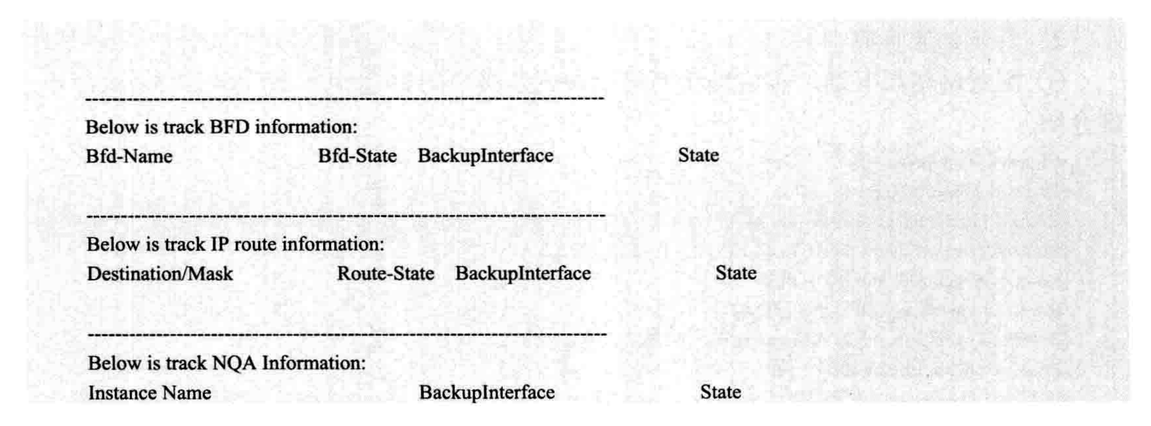
--------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask            Route-State   BackupInterface                State

--------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                          BackupInterface                State
```

在 ATM1/0/0 接口上执行 **shutdown** 命令，模拟链路故障，然后在 Router 上执行 **display standby state 命令**检查主备接口状态，可以看到 ATM1/0/0 的状态为 DOWN，备份接口 Cellular0/0/0 接口的状态为 UP，说明备份接口已被启用。

```
[Router-Atm1/0/0] shutdown
[Router-Atm1/0/0] quit
[RouterA] display standby state
Interface                     Interfacestate Backupstate Backupflag Pri    Loadstate
ATM1/0/0                                  DOWN          MDOWN              MU
Cellular0/0/0                           UP            UP            BU    0

 Backup-flag meaning:
 M---MAIN   B---BACKUP      V---MOVED      U---USED
 D---LOAD   P---PULLED
```


```
------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name                Bfd-State    BackupInterface              State

------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask           Route-State    BackupInterface              State

------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                    BackupInterface              State
```

9.3.4　以太链路+以太链路的接口备份与 BFD 联动配置示例

本示例的基本拓扑结构如图 9-7 所示，正常情况下，HostA 和 HostB 通过 RouterA、RouterB 和 RouterD 之间的链路作为主链路进行业务传输，RouterA、RouterC 和 RouterD 之间的链路作为备份链路。用户希望能在 50 ms 内检测到链路故障，并快速启用备份链路临时承担业务传输，以尽量减小主链路故障对业务传输的影响。

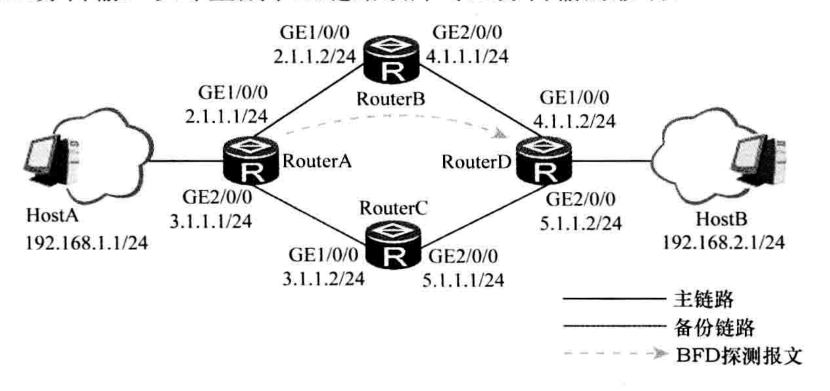


图 9-7　以太链路+以太链路接口备份与 BFD 联动配置示例拓扑结构

1. 基本配置思路分析

本示例要求实现毫秒级的主备接口快速切换，因此可采用接口备份与 BFD 联动功能来实现。在这里要特别注意的是，为了确保 HostA 和 HostB 主机之间的通信路径一致，需要在 RouterA 和 RouterD 两端同时配置接口备份与 BFD 联动功能。其基本配置思路如下。

① 配置各接口的 IP 地址及主备链路的静态路由，确认网络层互通。

② 分别在 RouterA 和 RouterD 上配置主链路对应的 BFD 会话，实现对主链路状态的检测。

③ 在 RouterA 的备份接口 GE2/0/0 上配置接口备份与 BFD 联动功能，以便在 BFD 检测到主链路故障时，流量可以快速切换到备份链路。

④ 在 RouterD 的备份接口 GE2/0/0 上配置接口备份与 BFD 联动功能，实现当 BFD 检测到主链路故障时，流量可以快速切换到备份链路，确保 RouterA 到 RouterD 的流量和 RouterD 到 RouterA 的流量选路保持一致。

2. 具体配置步骤

① 配置网络层互通。首先按组网需求配置各接口的 IP 地址，此处仅以 RouterA 为例介绍。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 2.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 3.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
```

然后在 RouterA 上配置去往 RouterD 的 4.1.1.0/24 和 5.1.1.0/24 两个网段的静态路由。注意**要配置备份链路的静态路由优先级更高（优先级值越小）**，以便故障时能正常切换。

```
[RouterA] ip route-static 4.1.1.0 255.255.255.0 2.1.1.2 preference 80
[RouterA] ip route-static 5.1.1.0 255.255.255.0 3.1.1.2 preference 60
```

同时，在 RouterD 上配置去往 RouterA 的 2.1.1.0/24 和 3.1.1.0/24 两个网段的静态路由。同样要配置备份链路的静态路由优先级更高（优先级值越小），以便故障时能正常切换。

```
[RouterD] ip route-static 2.1.1.0 255.255.255.0 4.1.1.1 preference 80
[RouterD] ip route-static 3.1.1.0 255.255.255.0 5.1.1.1 preference 60
```

② 配置 RouterA 到 RouterD 之间的 BFD 会话，注意这里需要双向配置。

下面是在 RouterA 上配置与 RouterD 之间的 BFD 会话。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd test bind peer-ip 4.1.1.2
[RouterA-bfd-session-test] discriminator local 10
[RouterA-bfd-session-test] discriminator remote 100
[RouterA-bfd-session-test] commit
[RouterA-bfd-session-test] quit
```

下面是在 RouterD 上配置与 RouterA 之间的 BFD 会话。

```
[RouterD] bfd
[RouterD-bfd] quit
[RouterD] bfd test bind peer-ip 2.1.1.1
[RouterD-bfd-session-test] discriminator local 100
[RouterD-bfd-session-test] discriminator remote 10
[RouterD-bfd-session-test] commit
[RouterD-bfd-session-test] quit
```

③ 在 RouterA 和 RouterD 的 GE2/0/0 上均配置接口备份与 BFD 联动。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby track bfd-session session-name test
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] standby track bfd-session session-name test
```

配置好后，在 RouterA 执行 **display bfd session all verbose** 命令，可看到 BFD 会话的状态为 Up。

```
[RouterA] display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 256          (Multi Hop) State :Up          Name : test
--------------------------------------------------------------------------------
  Local Discriminator      : 10          Remote Discriminator     : 100
```

```
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Peer Ip Address
Bind Session Type        : Static
Bind Peer Ip Address     : 4.1.1.2
Bind Interface           : -
FSM Board Id             : 0                 TOS-EXP               : 7
Min Tx Interval (ms)     : 1000              Min Rx Interval (ms)  : 1000
Actual Tx Interval (ms): 1000                Actual Rx Interval (ms): 1000
Local Detect Multi       : 3                 Detect Interval (ms)  : 3000
Echo Passive             : Disable           Acl Number            : -
Destination Port         : 3784              TTL                   : 254
Proc interface status    : Disable           Process PST           : Disable
WTR Interval (ms)        : -
Active Multi             : 3
Last Local Diagnostic    : No Diagnostic
Bind Application         : No Application Bind
Session TX TmrID         : -                 Session Detect TmrID  : -
Session Init TmrID       : -                 Session WTR TmrID     : -
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : -
--------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

在 RouterA 上通过执行 **display standby state** 命令查看 BFD 会话和备份接口的状态信息，可以看到 BFD 会话的状态是 UP，备份接口 GigabitEthernet2/0/0 的状态是 STANDBY。

```
<RouterA> display standby state
Interface                 Interfacestate Backupstate Backupflag Pri    Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP     V---MOVED     U---USED
 D---LOAD   P---PULLED


--------------------------------------------------------------------------
Below is track BFD Information:
Bfd-Name              Bfd-State   BackupInterface            State
test                    UP     GigabitEthernet2/0/0       STANDBY
--------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask           Route-State    BackupInterface            State

--------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                        BackupInterface              State
```

在 RouterB 的 GE2/0/0 接口执行 **shutdown** 命令，模拟链路故障，然后在 RouterA 上执行 **display bfd session all verbose** 命令，可以看到 BFD 会话的状态为 Down。

```
[RouterA] display bfd session all verbose
--------------------------------------------------------------------------
Session MIndex : 256          (Multi Hop) State :Down          Name : test
--------------------------------------------------------------------------
  Local Discriminator     : 10               Remote Discriminator    : 100
  Session Detect Mode     : Asynchronous Mode Without Echo Function
  BFD Bind Type           : Peer Ip Address
```

```
  Bind Session Type         : Static
  Bind Peer Ip Address      : 4.1.1.2
  Bind Interface            : -
  FSM Board Id              : 0                 TOS-EXP                : 7
  Min Tx Interval (ms)      : 1000              Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000                 Actual Rx Interval (ms): 1000
  Local Detect Multi        : 3                 Detect Interval (ms)   : 3000
  Echo Passive              : Disable           Acl Number             : -
  Destination Port          : 3784              TTL                    : 254
  Proc interface status     : Disable           Process PST            : Disable
  WTR Interval (ms)         : -
  Active Multi              : 3
  Last Local Diagnostic     : No Diagnostic
  Bind Application          : No Application Bind
  Session TX TmrID          : -                 Session Detect TmrID   : -
  Session Init TmrID        : -                 Session WTR TmrID      : -
  PDT Index                 : FSM-0|RCV-0|IF-0|TOKEN-0
  Session Description       : -
------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 0/1
```

此时再在 RouterA 上执行 **display standby state** 命令时，可看到此时 BFD 会话的状态是 ERR，备份接口 GigabitEthernet2/0/0 的状态是 UP，说明备份接口被启用。

```
<RouterA> display standby state
Interface                    Interfacestate Backupstate Backupflag Pri   Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP     V---MOVED     U---USED
 D---LOAD   P---PULLED


------------------------------------------------------------------------------
Below is track BFD Information:
Bfd-Name                  Bfd-State   BackupInterface               State
test                      ERR     GigabitEthernet2/0/0              UP
------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask          Route-State   BackupInterface             State

------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                      BackupInterface                  State
```

对 RouterB GE2/0/0 接口执行 **undo shutdown** 命令，GE2/0/0 接口恢复 UP 状态后，在 RouterA 上使用 **display standby state** 命令，可以看到此时 BFD 会话的状态是 UP，备份接口 GigabitEthernet2/0/0 又回到原来的 STANDBY 状态。输出示例略。

9.3.5　以太链路+以太链路的接口备份与 NQA 联动配置示例

本示例的拓扑结构可参见上节的图 9-7。正常情况下，HostA 和 HostB 间通过将 RouterA、RouterB 和 RouterD 之间的链路作为主链路进行业务传输，RouterA、RouterC 和 RouterD 之间的链路作为备份链路。现用户希望能实时监测主链路的网络状况，一旦检测到主链路出现故障，快速启用备份链路临时承担业务传输，以尽量减小主链路故障

对业务传输的影响。

本节的基本配置思路与上节的接口备份与 BFD 联动的配置类似，只是这里采用的是接口备份与 NQA 联动（**也需要在 RouterA 和 RouterD 上进行双向联动配置**），具体如下。

① 配置各接口的 IP 地址及主备链路的静态路由，确保网络层互通。

② 在 RouterA 上配置 ICMP 类型的 NQA 测试例，并在备份接口 GE2/0/0 上配置接口备份与 NQA 联动，以便当 NQA 检测到主链路故障时，流量可以快速切换到备份链路。

③ 在 RouterD 上配置 ICMP 类型的 NQA 测试例，并在备份接口 GE2/0/0 上配置接口备份与 NQA 联动，以便当 NQA 检测到主链路故障时，流量可以快速切换到备份链路。

通过以上两个方向的与 NQA 联动配置，可以确保 RouterA 到 RouterD 的流量和 RouterD 到 RouterA 的流量选路保持一致。

下面是具体的配置步骤。

① 配置网络层互通，要求配置各路由器接口和主、备链路在 RouterA 到 RouterD 之间的双向静态路由，与上节的第（1）步配置完全一样。

② 在 RouterA 和 RouterD 上分别配置 NQA 测试例，并与备份接口 GE2/0/0 进行联动。

下面是在 RouterA 上配置的 ICMP 类型 NQA 测试例与接口备份的联动。

```
[RouterA] nqa test-instance user test
[RouterA-nqa-user-test] test-type icmp
[RouterA-nqa-user-test] destination-address ipv4 4.1.1.2
[RouterA-nqa-user-test] frequency 10
[RouterA-nqa-user-test] probe-count 2
[RouterA-nqa-user-test] start now
[RouterA-nqa-user-test] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby track nqa user test
[RouterA-GigabitEthernet2/0/0] quit
```

下面是在 RouterD 上配置的 ICMP 类型 NQA 测试例与接口备份的联动。

```
[RouterD] nqa test-instance admin test
[RouterD-nqa-admin-test] test-type icmp
[RouterD-nqa-admin-test] destination-address ipv4 2.1.1.1
[RouterD-nqa-admin-test] frequency 10
[RouterD-nqa-admin-test] probe-count 2
[RouterD-nqa-admin-test] start now
[RouterD-nqa-admin-test] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] standby track nqa admin test
[RouterD-GigabitEthernet2/0/0] quit
```

配置好后，在 RouterA 上执行 **display nqa results test-instance** user test 命令，可以看到 NQA 测试实例的状态为 success。

```
[RouterA] display nqa results test-instance user test
NQA entry(user, test) :testflag is active ,testtype is icmp
  1 .Test 1 result    The test is finished
   Send operation times: 3                  Receive response times: 3
   Completion:success                         RTD OverThresholds number: 0
```

```
    Attempts number:1                         Drop operation number:0
    Disconnect operation number:0             Operation timeout number:0
    System busy operation number:0            Connection fail number:0
    Operation sequence errors number:0    RTT Stats errors number:0
    Destination ip address:4.1.1.2
    Min/Max/Average Completion Time: 60/90/80
    Sum/Square-Sum   Completion Time: 240/19800
    Last Good Probe Time: 2011-04-19 16:38:38.7
    Lost packet ratio: 0 %
```

然后在 RouterA 上通过 **display standby state** 命令查看 NQA 测试例和备份接口的状态信息，可以看到 NQA 测试例的状态是 OK，备份接口 GigabitEthernet2/0/0 的状态是 STANDBY（**参见输出信息粗体字部分**）。

```
<RouterA> display standby state
Interface                        Interfacestate Backupstate Backupflag Pri    Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP       V---MOVED       U---USED
 D---LOAD   P---PULLED


---------------------------------------------------------------------------
Below is track BFD Information:
Bfd-Name                    Bfd-State   BackupInterface                 State

-----------------------------------------------------------------------
Below is track IP route information:
Destination/Mask                Route-State   BackupInterface               State

-----------------------------------------------------------------------
Below is track NQA Information:
Instance Name                         BackupInterface                    State
user
test                                                                       OK
                                      GigabitEthernet2/0/0             STANDBY
```

对 RouterB 的 GE2/0/0 接口执行 **shutdown** 命令，模拟链路故障，然后在 RouterA 上执行 **display nqa results test-instance** user test 命令，可以看到 NQA 测试实例的状态为 failed（**参见输出信息粗体字部分**）。

```
[RouterA] display nqa results test-instance user test
NQA entry(user, test) :testflag is active ,testtype is icmp
  1 .Test 1 result    The test is finished
    Send operation times: 3                  Receive response times: 0
    Completion:failed                            RTD OverThresholds number: 0
    Attempts number:1                         Drop operation number:3
    Disconnect operation number:0             Operation timeout number:0
    System busy operation number:0            Connection fail number:0
    Operation sequence errors number:0    RTT Stats errors number:0
    Destination ip address:4.1.1.2
    Min/Max/Average Completion Time: 0/0/0
    Sum/Square-Sum    Completion Time: 0/0
    Last Good Probe Time: 0000-00-00 00:00:00.0
    Lost packet ratio: 100 %
```

再在 RouterA 上执行 **display standby state** 命令，可以看到此时 NQA 测试例的状态是 ERR，备份接口 GigabitEthernet2/0/0 的状态是 UP，说明备份接口被启用（**参见输出信息粗体字部分**）。

```
<RouterA> display standby state
Interface                     Interfacestate Backupstate Backupflag Pri   Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP      V---MOVED      U---USED
 D---LOAD   P---PULLED



------------------------------------------------------------------------
Below is track BFD Information:
Bfd-Name                  Bfd-State   BackupInterface                State

------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask             Route-State   BackupInterface               State

------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                          BackupInterface                  State
user
test                                                                      ERR
                                        GigabitEthernet2/0/0            UP
```

再对 RouterB 的 GE2/0/0 接口执行 **undo shutdown** 命令，GE2/0/0 接口恢复 UP 状态后，在 RouterA 上使用 **display standby state** 命令，可以看到此时 NQA 测试例的状态是 OK，备份接口 GigabitEthernet2/0/0 又回到原来的 STANDBY 状态。

同样也可以在 RouterD 上进行以上类似的测试和查看，不再赘述。

9.3.6　以太链路+以太链路的接口备份与路由联动配置示例

本示例的拓扑结构同样可参见 9.3.4 节的图 9-7。正常情况下，HostA 和 HostB 进行业务传输时，以 RouterA、RouterB 和 RouterD 之间的链路作为主链路，RouterA、RouterC 和 RouterD 之间的链路作为备份链路。现用户希望通过监控主链路路由状态方式检测主链路的连通状态，当主链路路由撤销或状态变为非激活时，快速启用备份接口临时承担业务传输，以尽量减小主链路故障对业务传输的影响。

1. 基本配置思路分析

因为静态路由没有收敛功能，仅支持接口备份与动态路由的联动，所以**本示例必须为主链路配置动态路由**（备链路可以是静态路由）。其基本的配置思路如下。

① 配置各接口 IP 地址。

② 在 RouterA、RouterB 到 RouterD 的主链路上配置 IS-IS 路由协议，使主链路各 Router 间路由可达。

③ 在 RouterA、RouterC 到 RouterD 的备份链路上配置缺省路由，使备份链路各 Router 间路由可达。

④ 在 RouterA 的备份接口 GE2/0/0 上配置接口备份与路由联动功能，当主链路的路

由撤销或者状态变为非激活时，启用备份接口，实现主备接口的快速切换。

2. 具体配置步骤

① 按组网需求配置各接口的 IP 地址，仅以 RouterA 为例进行介绍。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 2.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 3.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
```

② 在主链路各路由器上配置 IS-IS 协议，使能对应的 IS-IS 路由进程。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis enable 1
[RouterD] isis 1
[RouterD-isis-1] network-entity 10.0000.0000.0003.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis enable 1
```

配置好后，在 RouterA 执行 **display isis lsdb** 命令可看到 IS-IS LSDB 信息，具体如下。

```
[RouterA] display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                 Seq Num       Checksum     Holdtime     Length   ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x0000000d    0x61b6       797          96       0/0/0
0000.0000.0001.02-00* 0x00000003    0xaadf       797          55       0/0/0
0000.0000.0002.00-00  0x0000000e    0xa507       1124         84       0/0/0
0000.0000.0003.00-00  0x00000005    0xb274       250          68       0/0/0
0000.0000.0003.01-00  0x00000002    0xc5c2       250          55       0/0/0

Total LSP(s): 5
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload
```

在 RouterA 上执行 **display isis route** 命令查看路由信息，可以看到有路由可以正确到达 RouterD 的 4.1.1.0/24 网络。

```
[RouterA] display isis route

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface    NextHop          Flags
-------------------------------------------------------------------------------
2.1.1.0/24           10         NULL    GE1/0/0          Direct           D/-/L/-
4.1.1.0/24           20         NULL    GE1/0/0          2.1.1.2          A/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set
```

③ 在备份链路上配置 RouterA、RouterC 到 RouterD 链路间的静态路由。因为 RouterA 和 RouterD 中间只相隔一台路由器 RouterC，所以实际上就是配置 RouterA 和 RouterD 之间互通的双向静态路由。

```
[RouterA] ip route-static 5.1.1.0 255.255.255.0 3.1.1.2
[RouterD] ip route-static 3.1.1.0 255.255.255.0 5.1.1.1
```

④ 在 RouterA 的 GE2/0/0 上配置接口备份与路由联动。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby track ip route 4.1.1.0 255.255.255.0
```

配置完成后，在 RouterA 可以 Ping 通目的地址 4.1.1.2/24，结果证实是通的。然后，在 RouterA 上查看路由和备份接口的状态信息，可以看到到达目的网段 4.1.1.0/24 的路由状态是 OK，备份接口 GigabitEthernet2/0/0 的状态是 STANDBY（**参见输出信息粗体字部分**）。具体如下。

```
<RouterA> display standby state
Interface                   Interfacestate Backupstate Backupflag Pri    Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP     V---MOVED     U---USED
 D---LOAD   P---PULLED


-------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name               Bfd-State        BackupInterface              State

-------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask          Route-State   BackupInterface              State
4.1.1.0/24                OK              GigabitEthernet2/0/0          STANDBY

-------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                           BackupInterface              State
```

在 RouterB 的 GigabitEthernet2/0/0 接口上执行 **shutdown** 命令，模拟链路故障，然后在 RouterA 上执行 **display standby state** 命令，可以看到此时路由的状态是 ERR，备份接口 GigabitEthernet2/0/0 的状态是 UP，说明备份接口被启用（**参见输出信息粗体字部分**）。

```
<RouterA> display standby state
Interface                      Interfacestate Backupstate Backupflag Pri    Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP       V---MOVED      U---USED
 D---LOAD   P---PULLED


---------------------------------------------------------------------
Below is track BFD information:
Bfd-Name                   Bfd-State          BackupInterface              State

---------------------------------------------------------------------
Below is track IP route information:
Destination/Mask              Route-State    BackupInterface               State
4.1.1.0/24                    ERR            GigabitEthernet2/0/0          UP

---------------------------------------------------------------------
Below is track NQA Information:
Instance Name                                BackupInterface               State
```

最后，在 RouterB 的 GigabitEthernet2/0/0 接口上执行 **undo shutdown** 命令，GE2/0/0 接口恢复 UP 状态后，在 RouterA 上使用 **display standby state** 命令，可以看到此时路由的状态是 OK，备份接口 GigabitEthernet2/0/0 又回到 STANDBY 状态。

9.4 双机热备份基础

本章前面介绍的接口备份功能是为了解决同一设备上单一接口（或者说是单一链路）带来的单点故障问题，而本节介绍的双机热备份功能则是解决单一设备所带来的单点故障问题。因为在一些关键应用环境，如果只使用一台设备，无论其可靠性多高，网络都必然要承受因单点故障而导致业务中断的风险。

为了解决上述问题，引入了双机热备份（Hot-Standby Backup，HSB）。双机热备份实现了双机业务的备份功能，业务信息通过备份链路实现批量备份和实时备份，保证在主设备故障时业务能够不中断地顺利切换到备份设备，从而降低了单点故障的风险，提高了网络的可靠性。

9.4.1 双机热备份的备份方式

双机热备份是指当两台设备在确定主用（Master）设备和备份（Backup）设备后，由主用设备进行业务的转发，而备用设备处于监控状态，同时主用设备定时向备用设备发送状态信息和需要备份的信息。当主用设备出现故障后，备用设备及时接替主用设备的业务运行。

与上章介绍的 VRRP 以及本章前面介绍的接口备份一样，双机热备份也有两种不同的应用方式，即基本的主备方式和负载分担方式。

1. 主备方式

主备方式就是在正常情况下由主设备处理所有业务，并将产生的会话信息通过主备通道传送到备份设备进行备份；备份设备不处理业务，只用作备份。当主设备发生故障

时，备份设备会接替主设备处理业务。此时，由于已经在备用设备上备份了会话信息，从而可以保证新发起的会话能正常建立，当前正在进行的会话也不会中断，提高了网络的可靠性。当原来的主用设备故障恢复之后，用户可以根据需要配置是否将业务流量回切到原来的主用设备上。

2. 负载分担方式

负载分担方式是指使备份组中的各设备分别承担一部分用户流量，其实这与 VRRP 的负载分担方式是一样的。在图 9-8 所示的无线业务组网中，正常情况下，对于 AP1 上的业务流量，AC1 是主设备，AC2 是备份设备。AC1 处理所有业务，并将产生的会话信息通过主备通道传送到备份设备 AC2 进行备份；AC2 不处理业务，只用于备份。而对于 AP2 上的业务流量，AC2 是主设备，AC1 是备份设备。AC2 处理所有业务，并将产生的会话信息通过主备通道传送到备份设备 AC1 进行备份；AC1 不处理业务，只用于备份。这样，AP1 的业务流量通过 AC1 转发，AP2 的业务流量通过 AC2 转发，实现了流量的负载分担。

如果 AC1 发生故障，如图 9-9 所示，对于 AP1 上的业务流量，会自动切换到备份设备 AC2 上进行转发，保证了网络的可靠性。但是对于 AP2 上的业务流量，主用设备 AC2 正常工作，流量转发路径不变。当原来的主用设备故障恢复之后，用户可以根据需要配置是否将业务流量回切到原来的主用设备上。

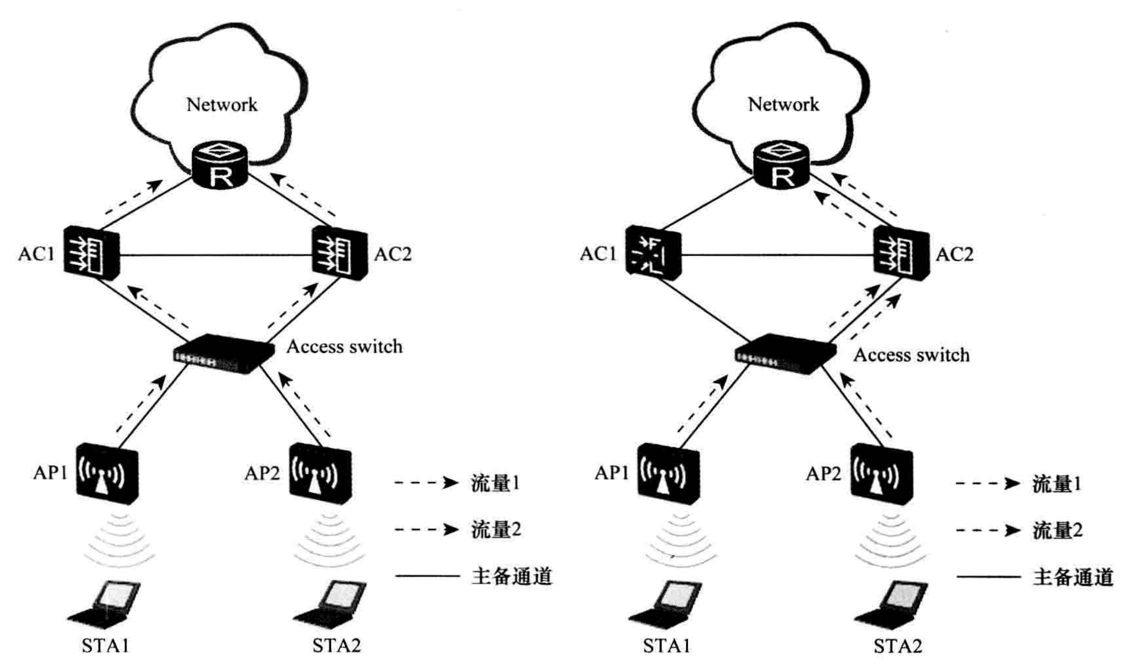


图 9-8　正常工作下的双机热备份负载分担示意图　　图 9-9　发生故障时的双机热备份负载分担示意图

9.4.2　双机热备份的实现机制

双机热备份功能的实现包括两个主要环节，即正常情况下进行的主、备设备上的数据同步，该环节保证主备设备信息一致；在主设备出现故障以及主设备故障恢复时的流量切换，该环节保证故障后业务能够不中断运行。

1. 数据同步机制

当主用设备出现故障，流量切换到备份设备时，要求主用设备和备份设备的会话表项完全一致，否则有可能导致会话中断。因此，需要一种机制在主用设备上会话建立或表项变化时能将相关信息同步保存到备份设备上。HSB 主备服务处理模块可以提供数据的备份功能，它负责在两个互为备份的设备间建立主备通道，并维护主备通道的链路状态，提供报文的收发服务。

数据同步的方式有批量备份和实时备份两种。

（1）批量备份

主用设备工作了一段时间后，可能已经存在大量的会话表项，此时加入备份设备，在两台设备上配置双机热备份功能后，先运行的主用设备会将已有的会话表项一次性同步到新加入的备份设备上，这个过程称为批量备份。

（2）实时备份

主用设备在运行过程中，可能会产生新的会话表项。为了保证与主备设备上表项的完全一致，主用设备在产生新表项或表项变化后会及时备份到备份设备上，这个过程称为实时备份。

2. 流量切换

双机热备份可以通过 VRRP 或双链路特性来实现流量的切换。其中 VRRP 只适用于主备备份方式，双链路可适用于主备备份和负载分担方式。**目前 AR G3 系列路由器仅支持通过 VRRP 来实现流量切换。**

（1）通过 VRRP 实现流量切换

通过 VRRP 实现流量切换要依靠 VRRP 功能，通过 HSB 主备业务备份组与 VRRP 备份组进行绑定，建立联动关系，然后根据 VRRP 备份组中的设备状态协商出热备设备业务的主备状态。即 **HSB 主备备份组的主备状态与 VRRP 的主备状态保持一致**，监控所绑定的主备通道状态和 VRRP 状态的变化，然后在主设备出现故障时，通知各个业务模块进行流量切换。

如图 9-10 所示，RouterA 和 RouterB 上配置了 VRRP 功能，其中 RouterA 配置为 VRRP 备份组的 Master 设备，RouterB 配置为 VRRP 备份组的 Backup 设备。双机热备份功能根据 VRRP 的主备状态协商出将 RouterA 作为双机热备份的主用设备，RouterB 作为双机热备份的备份设备（即双机热备份主备设备的选择与 VRRP 组主备设备的选择保持一致），HSB 主备服务会将主设备 RouterA 上的相关信息备份到备份设备 RouterB 上。

如果 RouterA 发生故障，如图 9-11 所示，VRRP 备份组会根据 VRRP 优先级选举 RouterB 成为 VRRP 备份组新的 Master 设备，进行业务流量的转发，从而实现了流量的切换。

（2）通过双链路实现流量切换

通过双链路实现流量切换与上面介绍的通过 VRRP 实现流量切换最大的不同就是这里不需要借助 VRRP 功能，不需要配置 VRRP 备份组，可直接利用双机热备份功能进行双链路状态的监测。

如图 9-12 所示，AP 与两个 AC 之间建立双链路，正常情况下，AC1 作为主设备，业务流量通过 AC1 进行转发。此时，双机热备份功能根据双链路的主备状态，协商出将 AC1 作为主设备，AC2 作为备份设备（即双机热备份主备设备的选择与双链路主备设备的选择保持一致）。HSB 主备服务会将主设备 AC1 上的相关信息备份到备份设备 AC2 上。

如果 AC1 发生故障，AP 感知到该故障，会自动将原来的备链路切换为主链路，AP

上的业务流量通过 AC2 进行转发，从而实现了流量的切换，如图 9-13 所示。

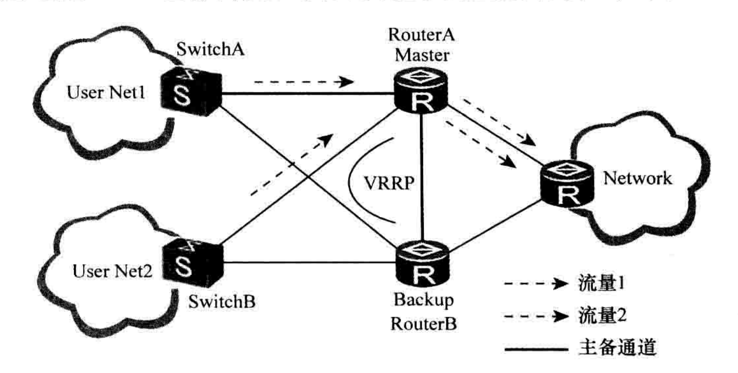


图 9-10　双机热备份通过 VRRP 实现流量切换前的示意图

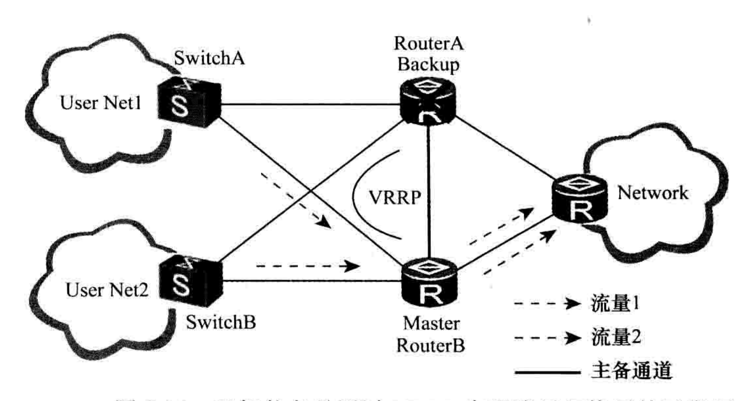


图 9-11　双机热备份通过 VRRP 实现流量切换后的示意图

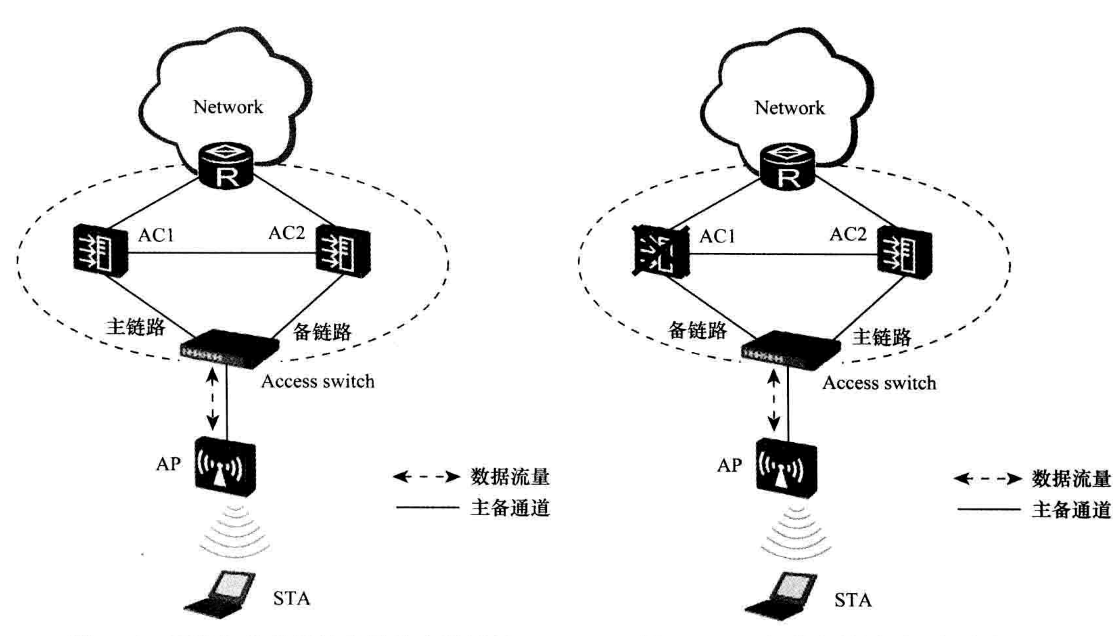


图 9-12　双机热备份通过双链路实现流量切换前的示意图

图 9-13　双机热备份通过双链路实现流量切换后的示意图

9.5 通过 VRRP 实现流量切换的双机热备份功能的配置与管理

本节介绍在AR G3系列路由器目前支持的通过VRRP实现流量切换的双机热备份功能。在这种流量切换实现机制中，需要同时配置 VRRP 备份组和 HSB 备份组，并且把 HSB 备份组与 VRRP 备份组进行绑定，实现 HSB 备份组设备的状态与 VRRP 备份组设备的状态同步一致。

通过 VRRP 实现流量切换的双机热备份功能的配置任务包括以下几种。

① 创建 HSB 主备服务。

② 配置 HSB 备份组。

③ 使能 HSB 备份组。

但在配置双机热备份功能之前，需要配置接口的网络层属性，使网络层路由可达，并配置好对应的 VRRP 备份组。有关 VRRP 备份组的配置方法参见本书第 8 章。

9.5.1 创建 HSB 主备服务

HSB 主备服务负责在两个互为备份的设备间建立主备备份通道，维护主备通道的链路状态，为其他业务提供报文的收发服务，并在备份链路发生故障时通知主备业务备份组进行相应的处理。

总体来说，HSB 主备服务主要包括两个方面。

① 建立主备备份通道：通过配置主备服务本端和对端的 IP 地址和端口号，建立主备机制报文发送的 TCP 通道，为其他业务提供报文的收发以及链路状态变化通知服务。

② 维护主备通道的链路状态：通过发送主备服务报文和重传等机制来防止 TCP 较长时间中断而协议栈没有检测到该连接中断的情况发生。它可以使当在主备服务报文时间间隔与重传次数乘积的时间内还未收到对端发送的主备服务报文时，设备会收到异常通知，并且准备重建主备备份通道。

说明 配置完成过后不能直接修改 HSB 主备备份通道参数，如果要进行修改，需要先删除 HSB 主备服务，再重新配置。但只有使能双机热备份功能后，配置的 HSB 主备服务报文的重传次数和发送间隔参数才会生效。

HSB 主备服务的配置步骤如表 9-5 所示（**需要同时在主、备设备上配置**）。

表 9-5　　HSB 主备服务的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**hsb-service** *service-index* 例如：[Huawei] **hsb-service** 0	创建 HSB 主备服务并进入 HSB 备份服务视图。参数 *service-index* 用来指定主备服务编号，**仅可为 0，即一个设备上仅可配置一个 HSB 主备服务**

（续表）

步骤	命令	说明
3	**service-ip-port local-ip** *local-ip-address* **peer-ip** *peer-ip-address* **local-data-port** *local-port* **peer-data-port** *peer-port* 例如：[Huawei-hsb-service-0] **service-ip-port local-ip** 192.168.1.1 **peer-ip** 192.168.1.2 **local-data-port** 10240 **peer-data-port** 10240	配置 HSB 主备服务的 IP 地址和端口号。命令中的参数说明如下 • *local-ip-address*：指定 HSB 主备服务绑定的本端 IP 地址 • *peer-ip-address*：指定 HSB 主备服务绑定的对端 IP 地址 • *local-port*：指定 HSB 主备服务绑定的本端端口号，取值范围 10 240～49 152 的整数 • *peer-port*：指定 HSB 主备服务绑定的对端端口号，取值范围 10 240～49 152 的整数 【说明】**这里所配置的本端和对端 IP 地址是指热备份的双机主备通道上两端设备直连接口上的 IP 地址**。HSB 主备备份通道参数必须在本端和对端同时配置，且本端的源 IP 地址、目的 IP 地址、源端口和目的端口分别为对端的目的 IP 地址、源 IP 地址、目的端口和源端口 缺省情况下，HSB 主备服务的 IP 地址和端口号未配置，可用 **undo service-ip-port** [**local-ip** *local-ip-address* **peer-ip** *peer-ip-address* **local-data-port** *local-port* **peer-data-port** *peer-port*]命令删除 HSB 主备服务配置的指定 IP 地址和端口号
4	**service-keep-alive detect retransmit** *retransmit-times* **interval** *interval-value* 例如：[Huawei-hsb-service-0] **service-keep-alive detect retransmit** 5 **interval** 1	（可选）配置 HSB 主备服务报文的重传次数和发送时间间隔。命令中的参数说明如下 • *retransmit-times*：指定 HSB 主备服务检测报文的重传次数，取值范围为 1～20 的整数 • *interval-value*：指定 HSB 主备服务检测报文的重传时间间隔，取值范围为 1～10 的整数秒 缺省情况下，HSB 主备服务报文的时间间隔为 3 s，重传次数为 5，可用 **undo service-keep-alive** [**detect retransmit** *retransmit-times* **interval** *interval-value*]命令恢复对应 HSB 主备服务报文的重传次数和发送间隔为默认值 【说明】HSB 主备服务报文的相关参数，包括发送时间间隔、重传次数在本端和对端都需要配置，且两端配置的参数值要保持一致

9.5.2　配置 HSB 备份组

HSB 主备业务备份组负责通知各个业务模块进行批量备份、实时备份和状态同步。各个业务备份功能依赖于业务备份组提供的状态协商和事件通知机制，实现业务信息的主备同步。

HSB 主备业务备份组依赖于 HSB 主备服务处理提供的主备通道，进行备份信息的同步，并响应主备服务处理的链路通断事件。需要为 HSB 备份组绑定 HSB 主备服务，才能使 HSB 备份组正常工作。此外，HSB 备份组还需要通过与 VRRP 备份组绑定，根据 VRRP 的状态协商出业务的主备状态；并通过监控所绑定的主备通道状态和 VRRP 状态的变化，通知各个业务模块进行批量备份、实时备份和状态同步。

HSB 备份组的配置步骤如表 9-6 所示（**需要同时在主、备设备上配置**）。

表 9-6 **HSB 备份组的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**hsb-group** *group-index* 例如：[Huawei] **hsb-group** 0	创建 HSB 备份组并进入 HSB 备份组视图。参数 *group-index* 用来指定主备备份组编号，**仅可为 0** 缺省情况下，设备上未创建 HSB 备份组，可用 **undo hsb-group** *group-index* 命令删除指定的 HSB 备份组
3	**bind-service** *service-index* 例如：[Huawei-hsb-group-0] **bind-service** 0	配置 HSB 备份组绑定的主备服务。参数 *service-index* 用来指定要绑定的 HSB 主备服务，**仅可为 0** 缺省情况下，HSB 备份组未绑定 HSB 主备服务，可用 **undo bind-service** *service-index* 命令删除 HSB 备份组绑定的指定的 HSB 主备服务
4	**track vrrp vrid** *vitual-router-id* **interface** *interface-type interface-number* 例如：[Huawei-hsb-group-0] **track vrrp vrid** 4 **interface** gigabitethernet 1/0/0	配置 HSB 备份组绑定的 VRRP 备份组。命令中的参数说明如下 ● *vitual-router-id*：指定 HSB 备份组要绑定的 VRRP 备份组编号，取值范围为 1～255 的整数 ● *interface-type interface-number*：指定当前设备中 VRRP 备份组所在的接口类型和接口编号 【说明】默认备份组中路由器采用抢占模式，抢占前要将原主设备上的数据批量备份到本设备。由于批量备份数据根据业务量多少需要一定的时间，为了保证主备切换时批量数据能够备份成功，不影响已有业务，在主设备的 VRRP 备份组上，先执行 **vrrp vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value* 命令配置抢占延时功能。要根据设备业务规格大小所需的批量备份时间配置适当的抢占延时，建议延时时间大于批量备份的时间 在实际组网中，确定上行链路可达的情况下，推荐执行 **vrrp vrid** *virtual-router-id* **preempt-mode disable** 命令设置备份组中路由器采用非抢占模式。在非抢占模式下，一旦备份组中的某台路由器成为 Master，只要它没有出现故障，其他路由器即使随后被配置更高的优先级也不会成为 Master 缺省情况下，HSB 备份组未绑定 VRRP 备份组，可用 **undo track vrrp** [**vrid** *vitual-router-id* **interface** *interface-type interface-number*] 命令删除 HSB 备份组绑定的指定的 VRRP 备份组
5	**quit** 例如：[Huawei-hsb-group-0] **quit**	退出 HSB 备份组视图，返回系统视图
6	**hsb-service-type firewall hsb-group** *group-index* 例如：[Huawei] **hsb-service-type firewall hsb-group** 0	（可选）使能防火墙主备功能，绑定主备备份组。参数 *group-index* 用来指定要绑定的 HSB 备份组编号，**只能为 0** 【说明】HSB 备份组使能（下节介绍）后不能进行业务功能与 HSB 备份组绑定的操作，请在使能 HSB 备份组前进行业务功能的绑定 缺省情况下，未使能防火墙主备功能，可用 **undo hsb-service-type firewall hsb-group** *group-index* 命令去使能防火墙主备功能

9.5.3　使能 HSB 备份组

HSB 备份组使能后，对 HSB 备份组的相关配置才会生效，HSB 备份组才会在状态发生变化时通知相应的业务模块进行处理。

使能 HSB 备份组的方法是在对应的 HSB 备份组视图下执行 **hsb enable** 命令。

9.5.4　双机热备份管理及典型故障排除

按照前面三节介绍的方法配置好双机热备份功能后，可以通过以下任意视图命令进行配置管理，以验证配置结果。

① **display hsb-group** *group-index*：查看指定 HSB 主备备份组的信息。

② **display hsb-service** *service-index*：查看指定 HSB 主备服务的信息。

另外，配置双机热备份后可能出现一些故障，如主备通道无法建立，主用设备上的信息无法正常备份到备份设备上，导致双机热备份功能不正常。

出现这种故障可能的原因主要有两个：一是两端主备通道参数配置不匹配，包括本端的源 IP 地址、源端口号和对端的目的 IP 地址、目的端口号不一致；二是两端主备服务报文的重传次数和重传间隔不一致。

这时，可先在任意视图下执行 **display hsb-service** *service-index* 命令，检查主用设备和备用设备上主备通道的参数配置是否匹配。

① 如果本端的源 IP 地址、源端口号和对端的目的 IP 地址、目的端口号不一致，则执行 **service-ip-port** local-ip *local-ip-address* **peer-ip** *peer-ip-address* **local-data-port** *local-port* **peer-data-port** *peer-port* 命令重新进行配置。

② 如果主用设备和备用设备上主备服务报文的重传次数和重传间隔不一致，则执行 service-keep-alive detect retransmit retransmit-times interval interval-value 命令重新进行配置。

9.5.5　配置双机热备份示例

本示例的基本拓扑结构如图 9-14 所示，用户网络通过 Switch 双线连接到 RouterA 和 RouterB。现用户希望实现，在正常情况下，用户网络内主机以 RouterA 为默认网关接入 Internet，RouterA 上的业务信息可以实现批量备份和实时备份到 RouterB 上；而当 RouterA 故障时，RouterB 接替 RouterA 继续进行工作，网络的运行不间断。

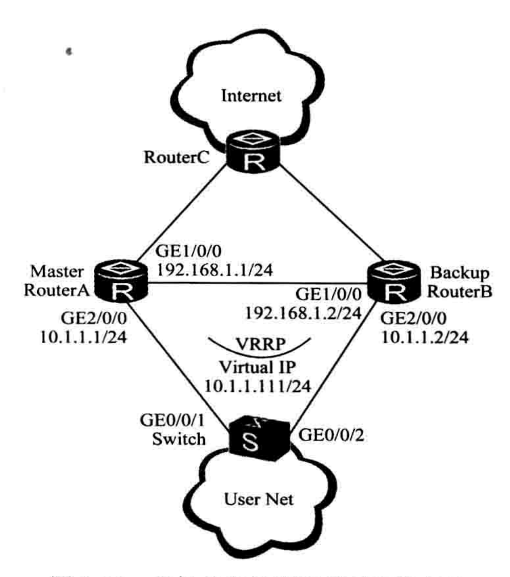


图 9-14　双机热备份配置示例拓扑结构

1. 基本配置思路分析

大家可能一看到这个要求就觉得很熟悉，这不是我们在上一章介绍的 VRRP 主备备份功能吗？是的，的确有太多相似之处，但这里有一个唯一的区别，那就是这里除了

要求进行主备备份外，还要求两个主用设备备份业务信息到备用设备上，所以在拓扑结构中，**两设备之间有一条用来建立主备通道的直连线，这是在 VRRP 主备备份中没有的**。

本章仅介绍了通过 VRRP 实现流量切换的配置方法，所以本示例也采用这种方案。根据本节前面介绍的配置方法，可以得出本示例的基本配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使各设备间网络层连通。

② 在 RouterA 和 RouterB 上分别配置 VRRP 备份组。其中，RouterA 上配置较高优先级，作为主用设备承担流量转发；RouterB 上配置较低优先级，作为备用设备。

③ 配置双机热备份功能，将 RouterA 上的业务信息通过链路批量备份和实时备份备份到 RouterB 上，保证在主设备故障时业务能够不中断地顺利切换到备份设备。

2. 具体配置步骤

① 配置设备各接口的 IP 地址，以 RouterA 为例。RouterB 的配置与之类似，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

② 配置 Switch 的二层透传功能，即把下面内网的 VLAN 数据报文以不带标签的方式向网关设备传输。

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port hybrid pvid vlan 100          !---指定接口的 PVID 为 VLAN 100
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 100      !---以不带标签方式允许 VLAN 100 报文通过，以实现 VLAN 报文上行二层透传
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port hybrid pvid vlan 100
[Switch-GigabitEthernet0/0/2] port hybrid untagged vlan 100
[Switch-GigabitEthernet0/0/2] quit
```

③ 在 RouterA 和 RouterB 上配置 VRRP 备份组，并指定 RouterA 具有更高的优先级，作为 Master 设备。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterB-GigabitEthernet2/0/0] quit
```

④ 在 RouterA 和 RouterB 上配置双机热备份功能，创建 HSB 主备服务和 HSB

备份组，并将 HSB 备份组与 HSB 主备服务和 VRRP 备份进行绑定，最后使能 HSB 功能。

```
[RouterA] hsb-service 0
[RouterA-hsb-service-0]service-ip-port local-ip 192.168.1.1 peer-ip 192.168.1.2 local-data-port 10241 peer-data-port 10241
[RouterA-hsb-service-0]quit
[RouterA] hsb-group 0
[RouterA-hsb-group-0]bind-service 0
[RouterA-hsb-group-0]track vrrp vrid 1 interface gigabitethernet 2/0/0
[RouterA-hsb-group-0] hsb enable
[RouterB] hsb-service 0
[RouterB-hsb-service-0] service-ip-port local-ip 192.168.1.2 peer-ip 192.168.1.1 local-data-port 10241 peer-data-port 10241
[RouterB-hsb-service-0]quit
[RouterB] hsb-group 0
[RouterB-hsb-group-0] bind-service 0
[RouterB-hsb-group-0] track vrrp vrid 1 interface gigabitethernet 2/0/0
[RouterB-hsb-group-0] hsb enable
```

完成上述配置以后，在 RouterA 和 RouterB 上分别执行 **display vrrp** 命令，可以看到 RouterA 在备份组中的状态为 Master，RouterB 在备份组中的状态为 Backup。

```
<RouterA> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State          : Master
    Virtual IP     : 10.1.1.111
    Master IP      : 10.1.1.1
    PriorityRun    : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2012-05-11 11:39:18 UTC-08:00
    Last change time : 2012-05-26 11:38:58 UTC-08:00
<RouterB> display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    State          : Backup
    Virtual IP     : 10.1.1.111
    Master IP      : 10.1.1.1
    PriorityRun    : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
```

```
Create time : 2012-05-11 11:39:18 UTC-08:00
Last change time : 2012-05-26 11:38:58 UTC-08:00
```

在 RouterA 和 RouterB 上分别执行 **display hsb-service** *service-index* 命令，可以看到 **Service State** 字段的显示为 **Connected**，说明主备服务通道已经成功建立。下面是 RouterA 上的输出示例。

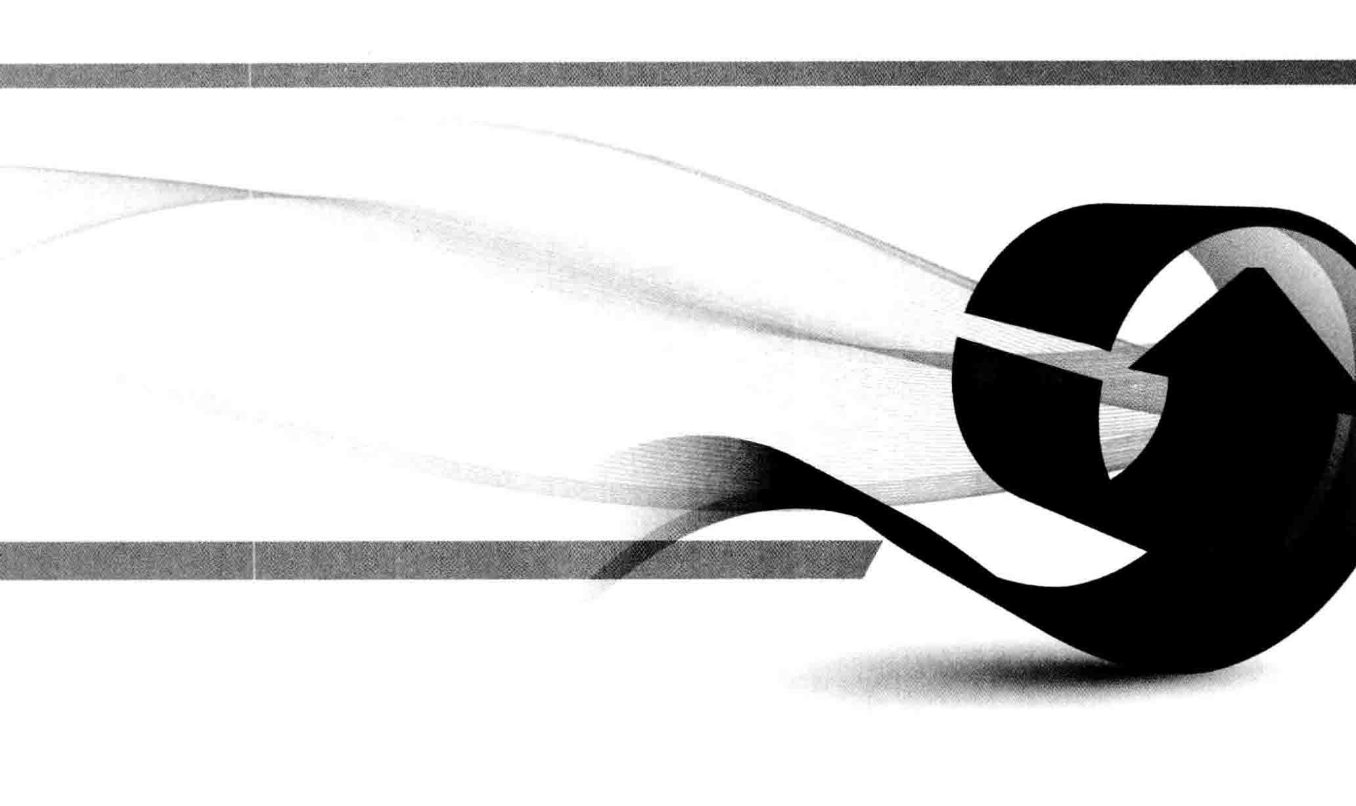
```
<RouterA> display hsb-service 0
Hot Standby Service Configuration:
----------------------------------------------------------
  Local IP Address          : 192.168.1.1
  Peer IP Address           : 192.168.1.2
  Source Port               : 10241
  Destination Port          : 10241
  Keep Alive Times          : 5
  Keep Alive Interval       : 3
  Service State             : Connected
  Service Batch Modules     :
----------------------------------------------------------
```

在 RouterA 和 RouterB 上分别执行 **display hsb-group** *group-index* 命令，可以看到 HSB 备份组当前为活跃状态，RouterA 为主用设备，RouterB 为备用设备。下面是 RouterB 上的输出示例。

```
<RouterB> display hsb-group 0
Hot Standby Group Configuration:
----------------------------------------------------------
  HSB-group ID              : 0
  Vrrp Group ID             : 2
  Vrrp Interface            : Vlanif100
  Service Index             : 0
  Group Vrrp Status         : Backup
  Group Status              : Active
  Backup Service Type       : Firewall
  Firewall Backup Process   :
```

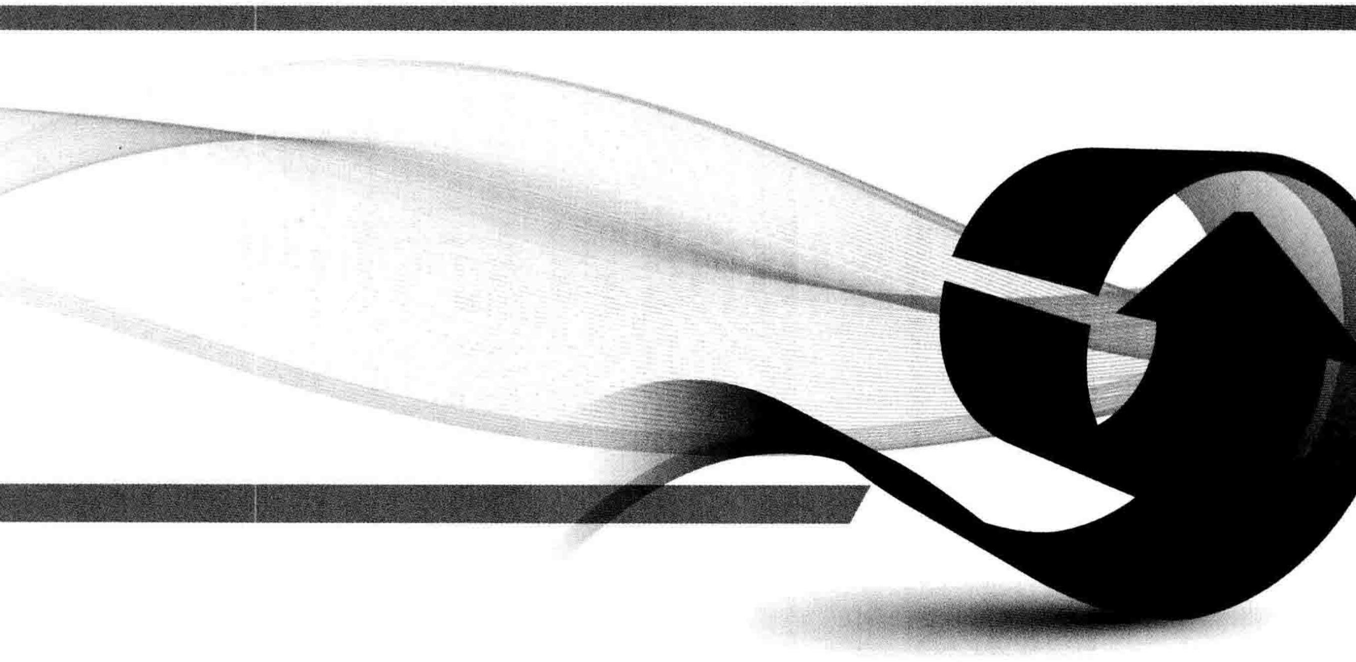
在 RouterA 的接口 GE2/0/0 和 GE1/0/0 上执行 **shutdown** 命令，模拟 RouterA 出现故障。然后在 RouterB 上执行 **display hsb-group** *group-index* 命令查看 HSB 备份组状态信息，可以看到 RouterB 已转换成 Master 状态，证明切换成功。

```
<RouterB> display hsb-group 0
Hot Standby Group Configuration:
----------------------------------------------------------
  HSB-group ID              : 0
  Vrrp Group ID             : 2
  Vrrp Interface            : Vlanif100
  Service Index             : 0
  Group Vrrp Status         : Master
  Group Status              : Active
  Backup Service Type       : Firewall
  Firewall Backup Process   :
```



第三篇

路由配置与管理



路由器的最主要功能当然就是为用户数据报文提供路由功能，所以本篇也是本书的重点与难点。本篇全面介绍了AR G3系列路由器的静态路由、RIP路由、OSPF路由、IS-IS路由以及策略路由和路由策略，具体包括以下几章内容。

- 第10意　静态路由配置与管理
- 第11章　RIP路由配置与管理
- 第12章　OSPF路由配置与管理
- 第13章　IS-IS路由配置与管理
- 第14章　BGP路由配置与管理
- 第15章　路由策略和策略路由配置与管理

至于以上这几种路由功能，相信大家都不陌生，在对应的章节中也有全面、深入的介绍，故在此不再赘述。本篇中最后一章讲的是路由策略和策略路由，虽然两者看起来有些相似，但其实它们的用途是完全不一样的。路由策略作用的是路由信息报文，用来进行路由信息接收和发送过滤，或者路由属性设置；而策略路由作用的是用户数据报文，用来进行用户数据报文过滤，或者控制用户数据报文的路由路径选择。

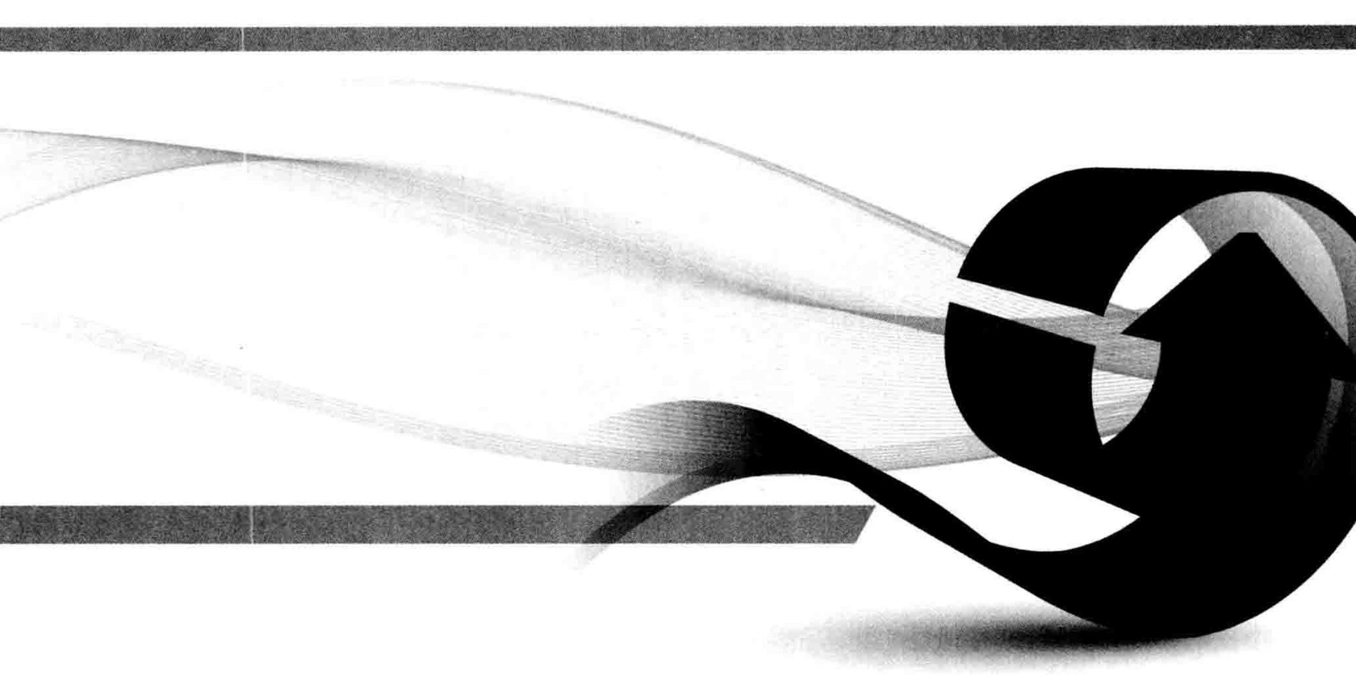
第10章
静态路由配置与管理

10.1 路由基础

10.2 静态路由基础

10.3 静态路由主要特性及应用

10.4 静态路由配置与管理



静态路由是一种最简单的路由，需要由管理员手动配置，主要用于小型网络，或者作为大中型网络中动态路由的补充。静态路由的配置很简单，用一条命令指定静态路由的目的IP地址、子网掩码、下一跳IP地址，或者出接口、优先级等主要参数值就可以了。另外，还可根据实际需要配置静态路由与BFD或者NQA的联动。

本章将先对路由、静态路由的主要基础知识（如路由的分类、路由表和转发表、路由协议的优先级、路由收敛和静态路由的组成等）、静态路由的主要特点进行深入的分析，然后具体介绍静态路由的各种特性配置与管理方法。同时辅以大量具体配置实例，以加深对这些基础知识和功能特性配置的理解。

10.1 路由基础

“路由”简单地说就是报文从源端到目的端的整条传输路径。当报文从路由器到目的网段有多条路由可达时，路由器可以根据路由表中最佳路由进行转发。最佳路由的选取与发现此路由的路由协议的优先级、所配置的路由度量有关。**当多条路由的协议优先级与路由度量都相同时，可以实现负载分担**，缓解网络压力；当多条路由的协议优先级与路由度量不同时，可以构成路由备份，提高网络的可靠性。

10.1.1 路由的分类

总体而言，根据路由的来源不同，可把路由分为以下三大类。

① 通过链路层协议发现的路由称为直连路由（Direct），**不需要配置**。

② 通过网络管理员手动配置的路由称为静态路由（Static）。

③ 通过动态路由协议发现的路由称为动态路由（分为RIP、OSPF、IS-IS、BGP等多种）。

“静态路由”是一种特殊的路由，因为它没有自己的路由算法，不能自动生成，纯粹依靠管理员为它们一级级地指明下一跳路径。也正因如此，所以静态路由的运行和维护都比较简单，但仅适用于拓扑结构简单并且稳定的小型网络，或者作为中大型网络中动态路由的补充，否则管理员的静态路由配置工作量会相当大，静态路由表项也可能非常多，甚至非常复杂。静态路由的另一个主要缺点就是不能自动适应网络拓扑的变化（即不具有主动网络收敛功能），需要人工干预。

“动态路由”相对“静态路由”来说就要“聪明”许多，因为它们都有自己的路由算法，能够根据用户配置自动生成对应的动态路由表项，且能够主动适应网络拓扑的变化。正因动态路由有这样的优势，所以动态路由更适用于具有一定数量三层设备的网络。

根据采用的不同路由算法，动态路由协议又有RIP（Routing Information Protocol，路由信息协议）、OSPF（Open Shortest Path First，开放最短路径优先）、IS-IS（Intermedia System-Intermedia System，中间系统到中间系统）和BGP（Border Gateway Protocol，边界网关协议）等。根据作用范围不同，这些动态路由协议可分为以下两种。

① IGP（Interior Gateway Protocol，内部网关协议）：在一个自治系统内部运行。常见的IGP包括RIP、OSPF和IS-IS。

② EGP（Exterior Gateway Protocol，外部网关协议）：运行于不同自治系统之间。目前常用EGP就是BGP。

根据使用的路由算法不同，以上这些动态路由协议又可分为以下两种。

① 距离矢量协议（Distance-Vector Protocol）：包括RIP和BGP。其中，BGP也被称为路径矢量协议（Path-Vector Protocol）。

② 链路状态协议（Link-State Protocol）：包括OSPF和IS-IS。

以上两种算法的主要区别在于发现路由和计算路由的机制不同。

说明 由于采用的算法不同，不同的路由协议可以发现不同的路由。当网络规模比较大，使用多种路由协议时，不同的路由协议间通常需要发布其他路由协议发现的路由，以实

现不同动态路由协议的不同网络的互通。

各动态路由协议都可以引入其他路由协议的路由，包括直连路由和静态路由，**但直连路由和静态路由不能引入其他类型的路由**。每种动态路由协议都有相应的路由引入机制，具体内容请参见各路由协议模块有关引入外部路由的描述。

10.1.2　路由表和 FIB 表

路由器在进行报文转发过程中要依据两种“表”——路由表（Routing Table）和 FIB（Forwarding Information Base，转发信息库）表。路由器通过路由表选择用于报文转发的路由，然后通过 FIB 表中的对应转发表项指导报文的转发。

1. 路由表

每台运行动态路由协议的路由器中都至少有两张“路由表”，一张是保存了所有最佳路由表项的本地核心路由表（即通常所说的 IP 路由表），另一张则是保存对应路由协议路由表项的协议路由表，如 RIP 路由表、BGP 路由表等。

（1）本地核心路由表

“本地核心路由表”用来保存本地路由器到达网络中各目的地的**当前各种最佳**（依据到达同一目的地的各种协议路由的优先级和度量值来选取优选路由）**协议路由**（包括直连路由、静态路由和各种动态路由），**只有到达某一目的地的最佳路由才会在本地核心路由表中出现，**并负责把这些最佳路由下发到 FIB 表，**生成对应的 FIB 表项**，指导报文的转发。

说明　对于支持 L3VPN（Layer 3 Virtual Private Network，三层 VPN）的路由器，每一个 VPN-Instance 拥有一个自己的本地核心路由表。

（2）协议路由表

协议路由表中存放着该协议已发现的所有路由信息，**但就所有路由表来说，协议路由表中的路由不一定是最佳路由，也就是说不一定会最终用来进行数据报文路由**。路由协议可以引入并发布其他协议生成的路由。例如，在路由器上运行 OSPF 协议，需要使用 OSPF 协议通告直连路由、静态路由或者 IS-IS 路由时，则要先将这些路由引入 OSPF 协议的路由表中。

在路由器中执行 **display ip routing-table** 命令时可查看路由器的 IP 路由表信息（**均为有效的最佳路由，非有效、最佳路由不会在 IP 路由表中显示**），如下所示。

```
<Huawei> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.137.216.1    GigabitEthernet 2/0/0
     10.10.10.0/24  Direct  0    0            D  10.10.10.10     GigabitEthernet 1/0/0
    10.10.10.10/32  Direct  0    0            D  127.0.0.1       InLoopBack0
   10.10.10.255/32  Direct  0    0            D  127.0.0.1       InLoopBack0
     10.10.11.0/24  Direct  0    0            D  10.10.11.1      LoopBack0
     10.10.11.1/32  Direct  0    0            D  127.0.0.1       InLoopBack0
```

```
   10.10.11.255/32  Direct  0    0        D   127.0.0.1        InLoopBack0
    10.137.216.0/23  Direct  0    0        D   10.137.217.208   GigabitEthernet   2/0/0
  10.137.217.208/32  Direct  0    0        D   127.0.0.1        InLoopBack0
  10.137.217.255/32  Direct  0    0        D   127.0.0.1        InLoopBack0
        127.0.0.0/8  Direct  0    0        D   127.0.0.1        InLoopBack0
       127.0.0.1/32  Direct  0    0        D   127.0.0.1        InLoopBack0
 127.255.255.255/32  Direct  0    0        D   127.0.0.1        InLoopBack0
 255.255.255.255/32  Direct  0    0        D   127.0.0.1        InLoopBack0
```

从以上 IP 路由表信息可以看出，IP 路由表中包含了下列字段。

① Destination：表示此路由的目的地址。用来标识 IP 包的目的地址或目的网络。

② Mask：表示此目的地址的子网掩码长度。与目的地址一起来标识目的主机或目的网络所在的网段地址。

③ Proto：表示学习此路由的路由协议，包括静态路由（Static）、直连路由（Direct）和各种动态路由。

④ Pre：即 Preference，表示此路由的路由协议优先级，具体参见 10.1.3 小节。**这是用来比较不同协议类型、相同目的地址的多条路由的优先级**。同一目的地可能存在不同下一跳、出接口等多条路由，这些不同的路由可能是由不同的路由协议发现的，也可以是手工配置的静态路由。优先级高（数值小）者将成为当前的最佳路由。

⑤ Cost：路由开销，**这是用来比较同一种协议类型、相同目的地址的多条路由的优先级**。但不同类型协议路由的开销类型不同，如距离矢量类协议采用的是“距离”，即将“跳数”作为路由开销，而链路状态类协议采用的是“链路状态”（由链路带宽、网络传输性能等参数共同决定）作为路由开销。当到达同一目的地的多条路由具有相同的路由优先级时，路由开销最小的将成为当前的最佳路由。

⑥ NextHop：表示此路由的下一跳 IP 地址。指明数据转发路径中的下一个三层设备。

⑦ Interface：表示此路由从本地设备发出的出接口。

在图 10-1 所示的网络中，路由器 A 与 3 个网络直接相连，因此在其 IP 路由表中有 3 个目的 IP 地址、下一跳和出接口的直连路由。

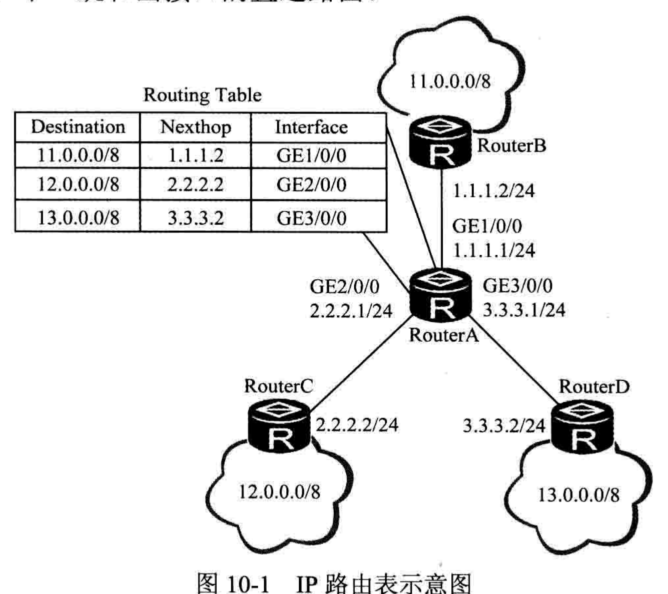


图 10-1 IP 路由表示意图

2. FIB 表的匹配

在 IP 路由表选择好要使用的路由表项后，IP 路由表会将这些路由表项下发到 FIB 表中，以生成对应的 FIB 表项（**所以 FIB 表中的表项是与 IP 路由表中的表项有对应关系的**）。当对应目的地址的报文到达路由器时，会通过查找 FIB 表中的对应表项进行转发。FIB 表中每条表项都指明到达某网段或某主机的报文应通过路由器的哪个物理接口或逻辑接口发送，这样就可到达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。可用 **display fib** 命令查看 FIB 表信息，如下所示。

```
<Huawei> display fib
FIB Table:
 Total number of Routes : 5
Destination/Mask    Nexthop         Flag TimeStamp     Interface              TunnelID
0.0.0.0/0           120.0.0.2       SU   t[37]         GigabitEthernet1/0/0   0x0
8.0.0.0/8           120.0.0.2       DU   t[37]         GigabitEthernet1/0/0   0x0
9.0.0.0/8           20.0.0.2        DU   t[9992]       GigabitEthernet3/0/0   0x0
9.1.0.0/16          120.0.0.2       DU   t[9992]       GigabitEthernet2/0/0   0x0
20.0.0.0/8          20.0.0.1        U    t[9992]       GigabitEthernet4/0/0   0x0
```

从中可以看出，在 FIB 表中包括 Destination、Mask、Nexthop、Flag、TimeStamp、Interface 和 TunnelID 字段，其中 Destination、Mask、Nexthop、Interface 字段是与 IP 路由表中的对应字段一样。其他 3 个字段说明如下。

① Flag：转发表项的标志，可能是 G、H、U、S、D、B、L 中一个或多字母的组合。

- G（Gateway 网关路由）：表示下一跳是网关。
- H（Host 主机路由）：表示该路由为主机路由。
- U（Up 可用路由）：表示该路由状态是 Up。
- S（Static 静态路由）：表示该路由为手动配置路由。
- D（Dynamic 动态路由）：表示该路由为根据路由算法自动生成路由。
- B（Black Hole 黑洞路由）：表示下一跳是空接口。
- L（Vlink Route）：表示 Vlink 类型路由。

② TimeStamp：转发表项的时间戳，表示该表项已存在的时间，单位是 s。

③ TunnelID：表示转发表项索引。该值不为 0 时，表示匹配该项的报文通过对应的隧道进行转发。该值为 0 时，表示报文不通过隧道转发。

因为在 IP 封装中，**IP 报头只封装了源 IP 地址和目的 IP 地址，没有封装对应的子网掩码**，所以这时如果在 FIB 表中有多条同时到达同一目的地，但处于相同自然网段的子网转发项时，就涉及最终选择哪条转发表的问题了。**这就是 FIB 表中的“最长掩码”匹配原则**，也即最精细路由匹配原则。具体方法是，在查找 FIB 表时，先将报文的目的地址**与 FIB 中各表项的掩码**按位进行“逻辑与”运算，得到匹配的网络地址（**可能有多个**），然后在这些对应的 FIB 表项中选择一个最长掩码的 FIB 表项进行报文转发。

例如，假设路由器上当前的 FIB 表如前所示，现有一个目的地址是 9.1.2.1 的报文进入路由器。首先，将目的地址 9.1.2.1 与 FIB 表中各表项的掩码长度“0、8、16”所对应的子网掩码进行“逻辑与”运算，得到下面几个网段地址：0.0.0.0/0、9.0.0.0/8、9.1.0.0/16。根据最长掩码匹配原则，最终会选择 9.1.0.0/16 表项从接口 GE2/0/0 转发这条目的地址是 9.1.2.1 的报文。

【经验之谈】 实际上 FIB 表项的选择没这么复杂，只需选择与报文中的目的地址第一个八位组相同的各子网和自然网段的转发表项，再加上所有缺省路由转发表项，然后从中选择子网掩码最长（最精细）的转发表项即可。

10.1.3 路由协议的优先级

对于相同的目的地，不同的路由协议（包括静态路由）可能会发现不同的路由，但这些路由并不都是最佳的。事实上，在某一时刻，到某一目的地的当前路由**仅能由唯一的路由协议来决定**。为了判断最佳路由，各路由协议都被赋予了一个优先级，当存在多个路由信息源时，具有较高优先级（**取值较小**）的路由协议发现的路由将成为最佳路由，并将最佳路由放入 IP 路由表中。

路由协议的优先级又分"外部优先级"和"内部优先级"两种。**选择路由时先比较路由的外部优先级，当不同的路由协议配置了相同的外部优先级时，系统才会通过内部优先级决定哪个路由协议发现的路由（内部优先级最高的）将成为最佳路由。**

外部优先级是指用户可以手动为各路由协议配置的优先级，我们通常所说的路由协议优先级就是指外部优先级。缺省情况下各路由协议的外部优先级如表 10-1 所示，优先级数值越小，表明其路由优先级越高。其中，0 表示直接连接的路由，255 表示任何来自不可信源端的路由，静态路由的优先级比 OSPF、IS-IS 中的路由优先级要低（**这点与 Cisco 中的不一样**）。除直连路由（DIRECT）外，各种路由协议的优先级都可由用户手动进行配置。

路由协议的内部优先级则不能被用户手动修改，**仅当到达同一目的地的多条路由的外部优先级相同时才会比较它们的内部优先级**。各路由协议的内部优先级如表 10-2 所示。

表 10-1 路由协议缺省时的外部优先级

路由协议的类型	路由协议的外部优先级
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	255
EBGP	255

表 10-2 路由协议内部优先级

路由协议的类型	路由协议的内部优先级
DIRECT	0
OSPF	10
IS-IS Level-1	15
IS-IS Level-2	18
STATIC	60

（续表）

路由协议的类型	路由协议的内部优先级
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	200
EBGP	20

例如，现有到达同一目的地 10.1.1.0/24 的两条路由可供选择，一条静态路由，另一条是 OSPF 路由，且这两条路由的外部优先级都被配置成 5。根据前面介绍的路由选择规则，这时路由器系统将根据内部优先级进行判断。因为 OSPF 协议的内部优先级是 10，高于静态路由的内部优先级 60，所以系统选择 OSPF 协议发现的路由作为最佳路由。

10.1.4　负载分担与路由备份

当多条路由的路由优先级和路由度量都相同时，这几条路由就称为等价路由，**多条等价路由可以实现负载分担。当几条路由为非等价路由时，就可以实现路由备份。**

1. 负载分担

路由器支持多路由模式，即允许配置多条目的地相同，且优先级也相同的路由。**当到达同一目的地存在同一路由协议发现的多条路由时，且这几条路由的开销值也相同，那么就满足负载分担的条件**。当实现负载分担时，路由器根据五元组（源 IP 地址、目的 IP 地址、源端口、目的端口、协议）进行转发。当五元组相同时，路由器总是选择与上一次相同的下一跳 IP 地址发送报文；而当五元组不同时，路由器会选取相对空闲的路径进行转发。

如图 10-2 所示，RouterA 已经通过接口 GE1/0/0 转发到目的地址 10.1.1.0/24 的第 1 个报文 P1，随后又需要分别转发报文到目的地址 10.1.1.0/24 和 10.2.1.0/24。其转发过程如下。

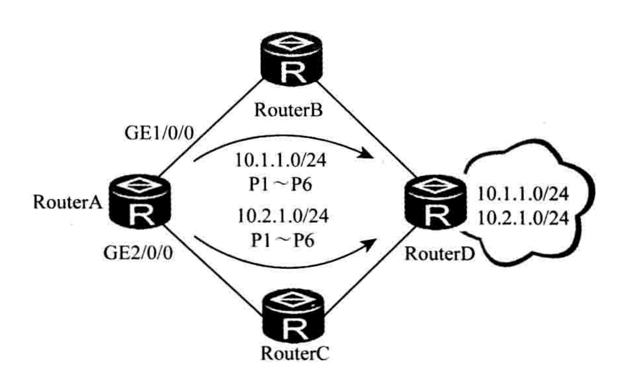


图 10-2　多路由负载分担示例

① 当转发到达 10.1.1.0/24 的第 2 个报文 P2 时，发现此报文与到达 10.1.1.0/24 的第 1 个报文 P1 的五元组一致，所以之后到达该目的地的报文都从 GE1/0/0 转发。

② 当转发到达 10.2.1.0/24 的第 1 个报文 P1 时，发现此报文与到达 10.1.1.0/24 的第 1 个报文 P1 的五元组不一致，所以选取从 GE2/0/0 转发，并且之后到达该目的地的报文都从 GE2/0/0 转发。

2. 路由备份

为了提高网络的可靠性，用户可以根据实际情况，配置到同一目的地的多条路由，其中一条路由的优先级最高，作为主路由，其余的作为备份路由。正常情况下，路由器采用主路由转发数据。当主链路出现故障时，主路由变为非激活状态，路由器选择备份路由中优先级最高的路由转发数据，这样就实现了主路由到备份路由的切换；而当主链路恢复正常时，由于主路由的优先级最高，路由器重新选择主路由来发送数据，这样就实现了从备份路由回切到主路由。

10.1.5 路由的收敛

路由收敛是指网络拓扑变化引起的通过重新计算路由而发生替代路由的行为。随着网络的融合，区分服务的需求越来越强烈。某些路由可能指导关键业务（如 VoIP，视频会议、组播等）转发，而这些关键的业务路由需要尽快收敛，而非关键路由可以相对慢一点收敛。因此，系统需要对不同路由按不同的收敛优先级处理，来提高网络可靠性。

按优先级收敛是指系统为路由设置不同的收敛优先级，从高到低分为 critical（临界）、high（高）、medium（中）、low（低）4 种。系统根据这些路由的收敛优先级采用相对的优先收敛原则，即按照一定的调度比例进行路由收敛安装，指导业务的转发。缺省情况下，公网路由收敛优先级如表 10-3 所示。对于私网路由，除了 OSPF 和 IS-IS 的 32 位主机路由标识为 medium 外，其余路由统一标识为 low。

表 10-3 缺省时的公网路由收敛优先级

路由协议或路由种类	收敛优先级
DIRECT	high
STATIC	medium
OSPF 和 IS-IS 的 32 位主机路由	medium
OSPF（除 32 位主机路由外）	low
IS-IS（除 32 位主机路由外）	low
RIP	low
BGP	low

如图 10-3 所示，网络上运行 OSPF 和 IS-IS 协议，组播接收者在 RouterA 端，组播源服务器 10.10.10.10/32 在 RouterB 端（有关 IP 组播请参见配套图书《**华为交换机学习指南**》），要求到组播服务器的路由优先于其他路由（例如 12.10.10.0/24）收敛。这时可以配置路由 10.10.10.10/32 的收敛优先级高于路由 12.10.10.0/24 的收敛优先级，这样当网络路由重新收敛时，就能确保到组播源的路由 10.10.10.10/32 优先收敛，保证组播业务的转发。

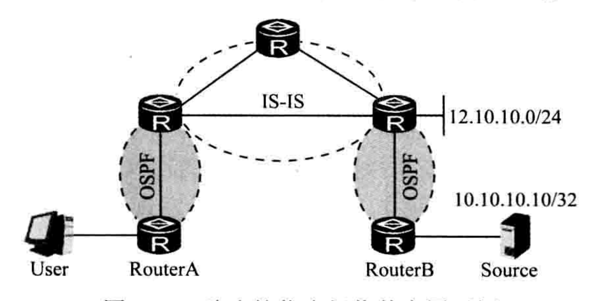


图 10-3 路由按优先级收敛应用示例

10.2 静态路由基础

静态路由是一种需要管理员手动配置的特殊路由。静态路由比动态路由使用更少的带宽，并且不占用 CPU 资源来计算和分析路由更新。但是，当网络发生故障或者拓扑发生变化后，静态路由不会自动更新，必须手动重新配置。

10.2.1 静态路由的组成

静态路由包括 5 个主要的参数：目的 IP 地址和子网掩码、出接口和下一跳 IP 地址、优先级。

1. 目的 IP 地址/子网掩码

目的 IP 地址就是路由要到达的目的主机或者目的网络的 IP 地址，子网掩码就是目的地址所对应的子网掩码。**当目的地址和掩码都为零时，表示静态缺省路由。**

2. 出接口和下一跳 IP 地址

根据不同的出接口类型，在配置静态路由时，可指定出接口，也可指定下一跳 IP 地址，还可以同时指定出接口和下一跳 IP 地址。

① 对于点到点类型的接口（如 PPP 链接接口），**只需指定出接口**。当然，也可同时指定下一跳 IP 地址，但这时已没有意义了。因为在点对点网络中，对端是唯一的，指定了发送接口即隐含指定了下一跳 IP 地址，这时认为与该接口相连的对端接口地址就是路由的下一跳 IP 地址。

② 对于 NBMA（Non Broadcast Multiple Access，非广播多路访问）类型的接口（如 FR、ATM 接口），**只需配置下一跳 IP 地址**。当然，也可同时指定出接口，但这时已没有意义了。因为除了配置 IP 路由外，这类接口还需在链路层建立 IP 地址到链路层地址的映射，相当于指定了出接口。

③ 对于广播类型的接口（如以太网接口）和 VT（Virtual-template）接口，**必须指定下一跳 IP 地址**，有些情况下还需要同时指定出接口。因为以太网接口是广播类型的接口，而 VT 接口下可以关联多个虚拟访问接口（Virtual Access Interface），这都会导致出现多个下一跳，无法唯一确定下一跳。而在广播型网络中，还可能有多个出接口到达同一个下一跳 IP 地址，此时就必须同时指定出接口。

3. 静态路由优先级

对于不同的静态路由，可以为它们配置不同的优先级。但要注意，优先级值越小表示静态路由的优先级越高。**配置到达相同目的地的多条静态路由，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份。**

10.2.2 静态路由的主要特点

正因为静态路由的配置比较简单，决定了静态路由包含了许多特点。在配置和应用静态路由时，我们应当全面地了解静态路由的以下几个主要特点。

1. 手动配置

静态路由需要管理员根据实际需要一条条手动配置，路由器不会自动生成所需的静

态路由。静态路由中包括目标节点或目标网络的 IP 地址，还可以包括下一跳 IP 地址、出接口，或者两者同时配置。

2. 路由路径相对固定

因为静态路由是手动配置的、静态的，所以每个配置的静态路由在本地路由器上的路径基本上是不变的，除非由管理员自己修改。另外，当网络的拓扑结构或链路的状态发生变化时，这些静态路由也不能自动修改，需要网络管理员手动修改路由表中相关的静态路由信息。

3. 不可通告性

静态路由信息在缺省情况下是私有的，不会主动通告给其他路由器，也就是当在一个路由器上配置了某条静态路由时，它不会被通告到网络中相连的其他路由器上。但网络管理员还是可以在本地设备的动态路由中引入静态路由，然后以对应动态协议路由进行通告，使得网络中其他路由器也可获此静态路由。

4. 单向性

静态路由是具有单向性的，也就是说它仅为数据提供沿着下一跳的方向进行路由，不提供反向路由。所以如果想要使源节点与目标节点或网络进行双向通信，就必须同时配置回程静态路由。在与读者朋友的交流中经常发现这样的问题，就是明明配置了到达某节点的静态路由，可还是 Ping 不通，其中一个重要原因就是没有配置回程静态路由。

如图 10-4 所示，如果想要使得 PC1（PC1 已配置了 A 节点的 IP 地址 10.16.1.2/24 作为网关地址）能够 Ping 通 PC2，则必须同时配置以下两条静态路由。

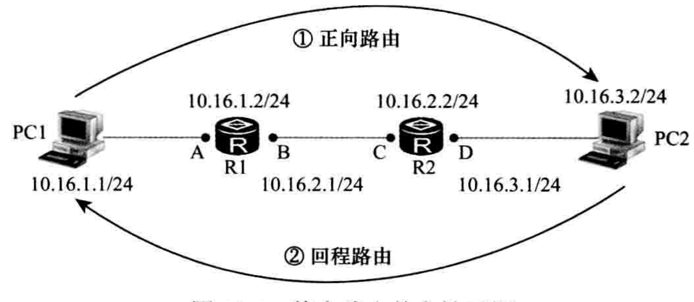


图 10-4 静态路由单向性示例

① 在 R1 路由器上配置了到达 PC2 的正向静态路由（以 PC2 10.16.3.2/24 作为目标节点，以 C 节点 IP 地址 10.16.2.2/24 作为下一跳 IP 地址）。

② 在 R2 路由器上配置到达 PC1 的回程静态路由（以 PC1 10.16.1.1/24 作为目标节点，以 B 节点 IP 地址 10.16.2.1/24 作为下一跳 IP 地址），以提供 Ping 过程回程 ICMP 消息的路由路径。

5. 接力性

如果某条静态路由中间经过的跳数大于 1（即整条路由路径经历了 3 个或 3 个以上路由器节点），则必须在除最后一个路由器外的其他路由器上依次配置到达相同目标节点或目标网络的静态路由，这就是静态路由的“接力”特性。

就像要从长沙到北京去，假设中间要途经的站点包括武汉、郑州、石家庄，可人家只告诉你目的地是北京以及从长沙出发的下一站是武汉。对于一个没有多少旅游经验的

人来说，你是不可能知道到了武汉后又该如何走，必须有人告诉你到了武汉后再怎么走，到了郑州后又该怎么走……这就是“接力性”。

图 10-5 所示为一个 3 个路由器串联的简单网络，各个路由器节点及 PC 的 IP 地址均在图中进行了标注，PC1 已配置好指向 R1 的 A 节点地址的网关，现假设要使 PC1 能 ping 得通 PC2，则需要在各路由器上配置以下 4 条静态路由（两条正向，两条回程）。

① 在 R1 路由器上配置了到达 PC2 的正向静态路由（以 PC2 10.16.4.0/24 作为目标节点，以 C 节点 IP 地址 10.16.2.2/24 作为下一跳 IP 地址）。

② 在 R2 路由器上配置了到达 PC2 的正向接力静态路由（同样以 PC2 10.16.4.0/24 作为目标节点，以 E 节点 IP 地址 10.16.3.2/24 作为下一跳 IP 地址）。

③ 在 R3 路由器上配置到达 PC1 的回程静态路由（以 PC1 10.16.1.1/24 作为目标节点，以 D 节点 IP 地址 10.16.3.1/24 作为下一跳 IP 地址），以提供 Ping 通信回程 ICMP 消息的路由路径。

④ 在 R2 路由器上配置到达 PC1 的回程接力静态路由（同样以 PC1 10.16.1.1/24 作为目标节点地址，以 B 节点 IP 地址 10.16.2.1/24 作为下一跳 IP 地址），以提供 Ping 通信回程 ICMP 消息的接力路由路径。

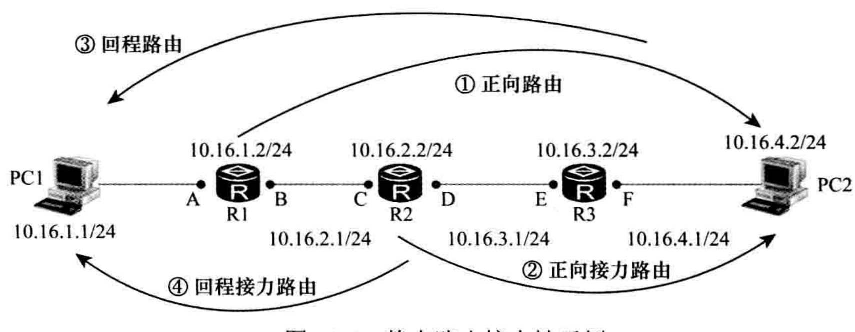


图 10-5　静态路由接力性示例

【经验之谈】路由器各端口上直接连接的各个网络都是直接互通的，因为它们之间缺省就有直连路由，因此无需另外配置其他路由。也即连接在同一路由器上的各网络之间的跳数为 0。如图 10-5 所示，R1 路由器上连接的 10.16.1.0/24 和 10.16.2.0/24 网络，R2 路由器上连接的 10.16.2.0/24 和 10.16.3.0/24 网络，R3 路由器上连接的 10.16.3.0/24 和 10.16.4.0/24 网络都是直接互通的。也正因如此，在图 10-4 中，PC1 要 ping 通 PC2，只需要配置图中所示的正、反向各两条静态路由，而不用配置从 R2 到 R3 路由器以及从 R2 到 R1 路由器的静态路由。

6. 迭代性

许多读者一直存在一个错误的认识，那就是认为静态路由的“下一跳”必须是与本地路由器直接连接的下一个路由器接口，其实这是错误的。前面说了，静态路由没有建立邻接关系的 Hello 包，静态路由也不会被通告邻居路由器，所以它的下一跳纯粹是由配置的“下一跳 IP 地址”直接指定的，或者通过配置的“出接口”间接指定。理论上来说，静态路由的下一跳可以是路径中其他路由器中的任意一个接口，只是能保证到达下一跳就行了。这就是静态路由的“迭代性”。

在图 10-5 所示的网络中，如果要在 R1 上配置一条到达 R3 所连接的 10.16.4.0/24 静态路由，按照正常思维的话，其下一跳应该是 R2 的 C 接口。不过，其实也可以是 R2 的 D 接口，或者 R3 的 E 接口，或者 F 接口。只要通过其他路由能到达这些接口，则这条静态路由就是成功的。

7. 适用小型网络

静态路由一般适用于比较简单的小型网络环境，因为在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。同时小型网络所需配置的静态路由条目不会太多，工作量也可以承受。如果网络规模较大，拓扑结构比较复杂，则不宜采用静态路由。

静态路由的缺点在于：它们需要在路由器上手动配置。因此，如果网络结构复杂，或者跳数较多的话，仅通过静态路由来实现路由，不仅要配置的静态路由可能非常多，而且还可能造成路由环路。另外，如果网络拓扑结构发生改变，路由器上的静态路由必须跟着改变，否则原来配置的静态路由将可能失效。

10.3 静态路由主要特性及应用

AR G3 系列路由器支持 IPv4 静态路由和 IPv6 静态路由，本书仅介绍 IPv4 路由。IPv4 静态路由的主要特性有静态缺省路由、静态路由与 BFD 联动、静态路由与 NQA 联动、静态路由优先级和静态路由永久发布。有关 BFD 和 NQA 的详细介绍参见第 7 章。

10.3.1 静态缺省路由

缺省路由是另外一种特殊的路由，分静态缺省路由和动态缺省路由两类。简单来说，缺省路由是没有在路由表中找到匹配的路由表项时才使用的候补路由。如果报文的目的地址不能与路由表的任何路由表项进行匹配，那么该报文将最终选取缺省路由尝试转发。如果路由器中没有配置缺省路由，且报文的目的地址不在路由表中，那么该报文将被丢弃，并向源端返回一个 ICMP 报文，报告该目的地址或网络不可达。

在路由表中，缺省路由以到网络 0.0.0.0（掩码也为 0.0.0.0）的路由形式出现。可通过命令 **display ip routing-table** 查看当前是否设置了缺省路由。通常情况下，管理员可以通过手动方式配置缺省静态路由；但有些时候，也可以使动态路由协议生成动态缺省路由，如 OSPF 和 IS-IS。

在图 10-6 中，如果不配置静态缺省路由，则需要在 RouterA 上配置到网络 3、4、5 的静态路由，在 RouterB 上配置到网络 1、5 的静态路由，在 RouterC 上配置到网络 1、2、3 的静态路由才能实现网络的互通。

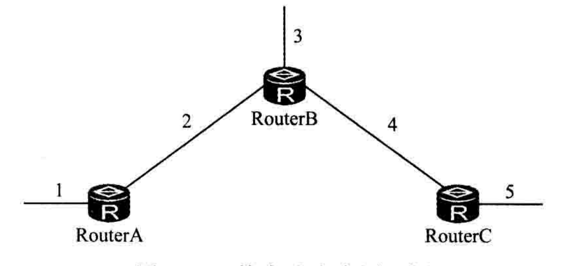


图 10-6 静态路由应用示例

如果配置缺省静态路由，因为 RouterA 发往 3、4、5 网络的报文下一跳都是 RouterB，

所以在 RouterA 上只需配置一条缺省路由，即可代替上个例子中通往 3、4、5 网络的 3 条静态路由。同理，RouterC 也只需要配置一条到 RouterB 的缺省路由，即可代替上个例子中通往 1、2、3 网络的 3 条静态路由。

10.3.2　静态路由与 BFD 联动

与动态路由协议不同，静态路由自身没有检测和网络收敛机制，当网络发生故障的时候，需要管理员介入。为了能提高故障发现的及时性，可通过静态路由与 BFD（双向转发检测）联动特性进行绑定，利用 BFD 会话来快速地检测静态路由所在链路的状态，实现毫秒级快速主、备链路切换。具体过程如下。

① 当某条静态路由上的 BFD 会话检测到链路故障时，BFD 会将故障上报系统，促使该路由失效，使该路由在 IP 路由表中不可见。

② 当某条静态路由上的 BFD 会话检测到故障的链路重新建立成功时，BFD 会上报系统，重新激活该路由，使该路由重新出现在 IP 路由表中。

有关 BFD 的详细介绍及配置方法参见第 7 章。

10.3.3　静态路由与 NQA 联动

在一些不支持 BFD 的链路环境中，可以通过把静态路由与 NQA（网络质量分析）特性进行绑定来实现链路故障检测和快速的主备链路切换，且只要求互通设备的其中一端支持 NQA 即可，不受二层设备的限制。在链路发生故障后，NQA 测试例可以快速地检测到链路的变化，并且在 IP 路由表中把与该 NQA 测试例联动的静态路由删除，从而影响流量的转发。静态路由与 NQA 联动特性的功能如下。

① 如果 NQA 测试例检测到链路故障，路由器将这条静态路由设置为“非激活”状态（此条路由不可用，从 IP 路由表中删除）。

② 如果 NQA 测试例检测到链路恢复正常，路由器将这条静态路由设置为“激活”状态（此条路由可用，添加到 IP 路由表）。

注意　静态路由与 NQA 联动时仅采用 ICMP 测试例来检测源端到目的端的路由是否可达，且每条静态路由只可以绑定一个 NQA 测试例。有关 NQA 的详细介绍参见本书第 7 章。

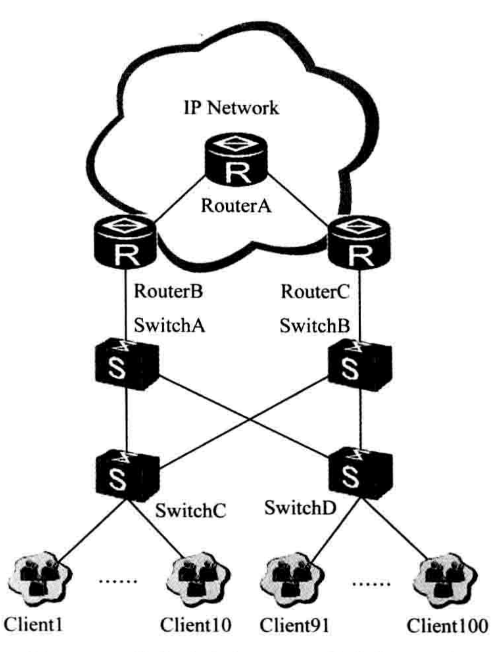


图 10-7　静态路由与 NQA 联动应用示例

如图 10-7 所示，每台接入交换机下连接 10 个用户，共 100 个用户。由于在 RouterB 和用户之间无法使用动态路由协议，所以在 RouterB 上配置到用户的静态路由。出于网络稳定性的考虑，在 RouterC 上进行同样的配置，作为冗余备份。RouterA、RouterB 和 RouterC 上运行动态路由协议，相互间可以学习路由。其中，RouterB 和 RouterC 配置动态路由

协议引入静态路由，并且设置不同的度量值，这样 RouterA 也能通过动态路由协议从 RouterB 和 RouterC 分别学习到用户的路由，RouterA 根据两条链路的度量值不同选择一条主用链路，另一条链路做为备份链路。

在 RouterB 上配置静态路由与 NQA 联动特性，利用 NQA 测试例检测主用链路 RouterB→SwitchA→SwitchC（SwitchD）的状态，当主用链路发生故障时，撤销静态路由发布，使下行流量经无故障的链路 RouterC→SwitchB→SwitchC（SwitchD）转发。在两条链路都正常时，控制下行流量优先选择主用链路。

10.3.4 静态路由优先级

可以为不同静态路由配置不同的优先级，优先级值越小，对应的静态路由优先级越高。通过为多条到达同一目的地址的静态路由配置相同或不同的优先级，则又可分别实现多条相同目的地址的静态路由的负载分担和路由备份。

1. 负载分担

如果为到达相同目的地址的多条静态路由指定相同优先级，则可实现负载分担。如图 10-8 所示，从 RouterA 到 RouterC 有两条优先级相同的静态路由，此时两条路由都会出现在路由表上，同时进行数据的转发。

2. 路由备份

如果为多条到达相同目的地的多条静态路由指定不同优先级，则可实现路由备份。如图 10-9 所示，从 RouterA 到 RouterC 有两条优先级不同的静态路由。下一跳是 RouterB 的静态路由 B 的优先级较高，该路由所在链路作为主链路。下一跳是 RouterD 的静态路由 D 的优先级较低，作为备份路由，该路由所在链路作为备份链路。

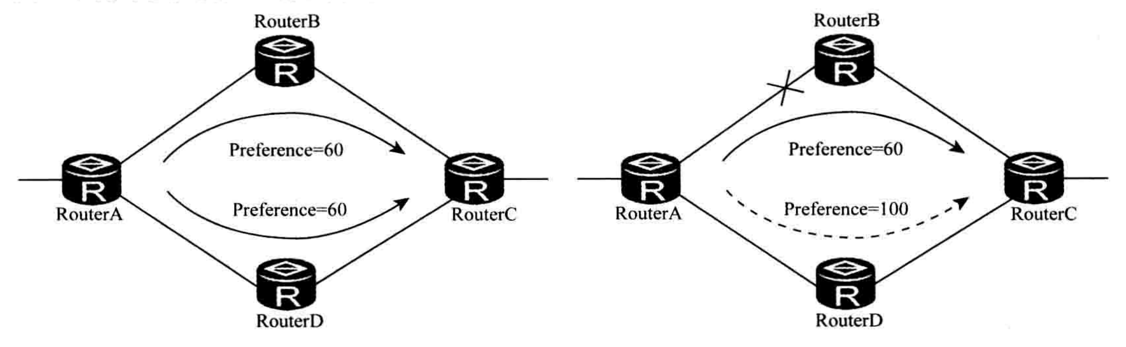


图 10-8 多条静态路由的负载分担应用示例　　图 10-9 多条静态路由的路由备份应用示例

在正常情况下，静态路由 B 被激活，主链路承担数据转发业务。静态路由 D 不在路由表中体现。

① 在主链路上出现故障时，静态路由 B 在路由表中被删除，而静态路由 D 则作为备份路由被激活，备份链路承担数据转发业务。

② 在主链路恢复正常后，静态路由 B 重新被激活，主链路承担数据转发业务。而静态路由 D 作为备份路由，在路由表中删除。因此这条备份路由也叫**浮动静态路由**。

10.3.5 静态路由永久发布

链路有效性直接影响网络的稳定性和可用性，因此链路状态的检测对网络维护具有

重要意义。BFD 作为一种常用方案，并不适合所有的场景。例如，在不同的 ISP 之间，客户希望采用更简单、更自然的方式来达到这一目的。

静态路由永久发布可以为客户提供一种低成本、部署简单的链路检测机制，并提高与其他厂商设备的兼容性。在客户希望确定业务流量的转发路径，不希望流量从其他路径穿越时，静态路由永久发布可以通过 Ping 静态路由目的地址的方式来检测链路的有效性而达到业务监控的目的。配置永久发布属性后，之前无法发布的静态路由仍然被优选并添加到 IP 路由表中。具体可以分为以下两种情况。

① 静态路由配置了出接口，且出接口的 IP 地址存在时，无论出接口的状态是 Up 还是 Down，只要配置了永久发布属性，则该静态路由都会被优选并添加到 IP 路由表。

② 静态路由没有配置出接口时，无论静态路由是否能迭代到出接口，只要配置了永久发布属性，路由都会被优选并添加到 IP 路由表中。

这样，通过控制静态路由的优先级和前缀长度，使 Ping 报文始终通过静态路由转发，就可以检测出链路的有效性。但是，该特性不判断路由是否可达，而是一直会将静态路由保留在 IP 路由表中，如果实际路径不可达，静态路由可能形成黑洞路由。

如图 10-10 所示，BR1、BR2 和 BR3 分别属于 ISP1、ISP2 和 ISP3。从 BR1 到 BR2 有两条链路（LinkA 和 LinkB）可达，但 ISP1 希望业务流量都通过 LinkA 直接转发到 ISP2，而不从 ISP3 穿越。这时就可以配置 ISP1 到 ISP2 的静态路由为永久发布的。

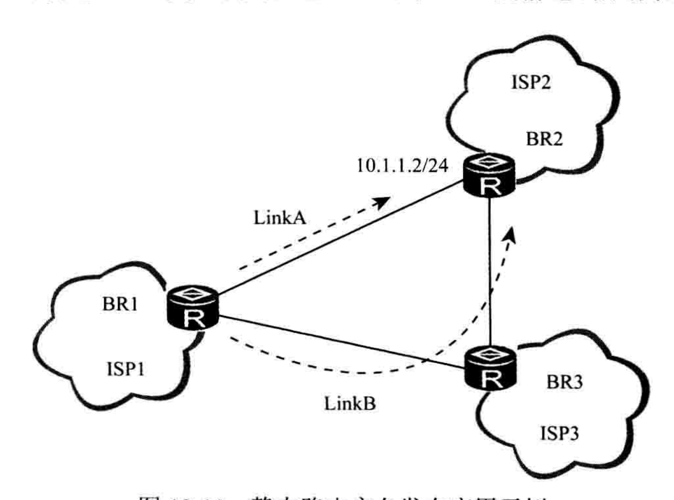


图 10-10　静态路由永久发布应用示例

此时，在 BR1 和 BR2 之间建立直连单跳 EBGP 邻居，同时为了进行业务状态监控，在 BR1 上配置到对端（BR2）BGP 邻居地址（10.1.1.2/24）的静态路由（出接口为与 BR2 直连的本地接口），并使能路由永久发布。网络监控系统周期性地 Ping 10.1.1.2，可通过 Ping 结果来判断 LinkA 的状态，进而间接地监控 BGP 业务状态。

当 LinkA 正常时，Ping 数据包都通过 LinkA 进行转发。如果 LinkA 发生故障，即使能通过 LinkB 到达 BR2，但由于静态路由使能了静态路由永久发布，所以 Ping 数据包还是通过 LinkA 进行转发，但此时转发不通。对于 BGP 数据包也是相同的情况，故障会导致 BGP 邻居断开，监控系统可以通过 Ping 结果间接地检测到业务问题，并通知维护人员及时响应。

10.4 静态路由配置与管理

根据 10.2.3 小节介绍的 AR G3 系列路由器静态路由特性，可以得出如下整个静态路由（**本书仅介绍 IPv4 静态路由**）的主要配置（仅第一项是必选的，其他可选项的配置是并列关系，可根据实际需要选择配置）。

① 创建静态路由。

②（可选）配置静态路由的缺省优先级。

③（可选）使能静态路由按递归深度优先选择。

④（可选）配置静态路由永久发布。

⑤（可选）静态路由与静态 BFD 联动。

⑥（可选）静态路由与静态 NQA 联动。

以上 6 项配置任务中，前面 4 项为基本功能配置，后面两项是静态路由与其他技术的联动配置。下面分别予以介绍。

10.4.1 配置静态路由基本功能

静态路由基本功能包括以下配置任务。

（1）创建静态路由

在创建静态路由时，可以同时指定出接口和下一跳。对于不同的出接口类型，也可以只指定出接口或只指定下一跳。

① 对于点到点接口，**只需指定出接口**（可同时指定下一跳）。

② 对于 NBMA 接口，**只需指定下一跳**（可同时指定出接口）。

③ 对于以太网接口和 VT 接口，**必须指定下一跳**（有时需同时指定出接口）。

说明 在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是静态缺省路由。缺省情况下，没有创建静态缺省路由。

（2）（可选）配置静态路由的缺省优先级

静态路由有缺省优先级值（60），也可以改变其缺省优先级，以影响路由的选路顺序。在配置静态路由时，如果没有专门指定优先级，就会使用缺省优先级。

（3）（可选）使能静态路由按递归深度优先选择

路由迭代是通过路由的下一跳信息来找到直连出接口的过程。迭代深度指路由迭代中查找路由的次数，次数越少迭代深度越小。当系统中存在若干条同一前缀，但迭代深度不同的静态路由时，迭代深度较小的路由稳定性较高。配置了基于迭代深度的优选之后，系统会选择迭代深度较小的静态路由作为活跃路由，并下发 FIB，其他路由为不活跃路由。

（4）（可选）配置静态路由永久发布

静态路由永久发布就是通过 Ping 静态路由目的地址的方式来检测链路的有效性。配置静态路由永久发布后，静态路由会一直生效，不受路由出接口状态的影响。

以上这 4 项配置任务的具体配置步骤如表 10-4 所示（创建静态路由时要区分是在公共网络中创建，还是在具体的 VPN 实例网络中创建，而且不同类型网络中所允许携带的参数不完全相同）。

表 10-4　静态路由基本功能配置步骤

步骤	命令		说明
1	**system-view** 例如：< Huawei > **system-view**		进入系统视图
2	**在 NBMA 或者广播网络中：** **ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-instance-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * [**description** *text*] **在点对点网络中：** **ip route-static** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference***preference* | **tag** *tag*] * **ldp-sync** [**description** *text*] 例如：[Huawei] **ip route-static** 10.1.1.0 24 172.16.0.1 GigabitEthernet2/0/0	（二选一）在公网（即非特定 VPN 实例的网络）上配置静态路由	命令中的参数和选项说明如下 ● *ip-address* 或 *destination-address*：指定静态路由的目的 IP 地址，**可以是主机 IP 地址（创建主机静态路由时），也可以是网络 IP 地址（创建网络静态路由时）** ● *mask* | *mask-length*：指定静态路由的目的 IP 地址所对应的子网掩码（选择 *mask* 参数时）或子网掩码长度（选择 *mask-length* 参数时）。**如果创建的是主机静态路由，子网掩码为 255.255.255.255，对应的子网掩码长度为 32**。如果目的 IP 地址和掩码都为 0.0.0.0，则配置的路由为缺省路由 ● *nexthop-address*：多选一参数，指定静态路由的下一跳 IP 地址 ● **public**：可选项，指定 *nexthop-address* 参数值是公网地址，而不是源 VPN 中的 IP 地址。在为 VPN 实例配置静态路由时，下一跳 IP 地址可以属于 VPN 实例，也可以属于公网。如果是公网的，则必须选择此可选项 ● *interface-type interface-number* [*nexthop-address*]：多选一参数，指定静态路由的出接口，或同时选择指定静态路由的下一跳 IP 地址 ● **vpn-instance** *vpn-instance-name nexthop- address*：多选一参数，指定静态路由在由参数 *vpn-instance-name* 指定的 VPN 实例中的下一跳 IP 地址。如果指定了 VPN 实例的名称，静态路由将根据配置的 *nexthop-address* 在 VPN 实例路由表中查找出接口 ● **vpn-instance** *vpn-source-name*：指定源 VPN 实例的名称，1～31 个字符，区分大小写，不支持空格。配置的静态路由将被加入指定 VPN 实例的路由表中 ● **vpn-instance** *vpn-destination-name*：多选一参数，指定目的地址所在接口绑定的 VPN 实例，1～31 个字符，区分大小写，不支持空格 ● **preference** *preference*：可多选参数，指定静态路由的优先级，取值范围为 1～255 的整数，缺省值是 60 ● **tag** *tag*：可多选参数，指定静态路由的 tag 属性值，取值范围为 1～4 294 967 295 的整数，缺省值是 0。配置不同的 tag 属性值，可对静态路由进行分类，以实现不同的路由管理策略。例如，其他协议引入静态路由时，可通过路由策略引入具有特定 tag 属性值的路由。**有关路由策略的详细介绍和配置参见第 15 章**

（续表）

步骤	命令	说明	
2	在 NBMA 或者广播网络中： **ip route-static vpn-instance** *vpn-source-name destination-address* { *mask* | *mask-length* } { *nexthop-address* [**public**] | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-destination-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * [**description** *text*] 在点对点网络中： **ip route-static vpn-instance** *vpn-source-name destination-address*{ *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync** [**description** *text*] 例如：[Huawei] **ip route-static vpn-instance** vpn1 10.1.1.0 24 **vpn-instance** vpn2 1.1.1.2	（二选一）在VPN实例中配置静态路由	• **ldp-sync**：使能 LDP（标签分发协议）和静态路由同步功能 • **description** *text*：可选参数，配置静态路由的描述信息，1～35 个字符，支持空格 缺省情况下，系统没有配置任何单播静态路由，左边这四条命令分别对应可用 **undo ip route-static** *ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag***tag*] *，或者 **undo ip route-static** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync**，或者 **undo ip route-static vpn-instance** *vpn-source-name destination-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] *，或者 **undo ip route-static vpn-instance** *vpn-source-name destination-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * [**ldp-sync**]命令删除指定的静态路由，也可用 **undo ip route-static all** 或者 **undo ip route-static vpn-instance** *vpn-source-name* **all** 命令删除公网中或者指定 VPN 实例中的所有静态路由
3	**ip route-static default-preference** *preference* 例如：[Huawei]**ip route-static default-preference** 70	（可选）设置静态路由的缺省优先级，取值范围为 1～255 的整数。缺省优先级配置将**仅在所有上一步在创建静态路由时没有指定** *preference* **参数值的静态路由上生效** 缺省情况下，IPv4 静态路由的缺省优先级是 60，可用 **undo ip route-static default-preference** 命令恢复静态路由的缺省优先级的缺省值	
4	**ip route-static selection-rule relay-depth** 例如：[Huawei]**ip route-static selection-rule relay-depth**	（可选）使能静态路由按迭代深度进行优选功能。配置了基于迭代深度优选之后，静态路由模块会选择迭代深度较小的静态路由作为活跃路由，并下发 FIB 表，可能会使原来活跃的路由变为不活跃 缺省情况下，没有使能静态路由按迭代深度优选功能，可用 **undo ip route-static selection-rule relay-depth** 命令去使能静态路由按迭代深度进行优选功能	
5	**ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-instance-name nexthop-address* } **permanent** 例如：[Huawei] **ip route-static** 10.1.1.0 **permanent**	（可选）配置静态路由永久发布。命令中的参数说明参见前面第 2 步对应的参数说明 缺省情况下，系统没有配置任何永久发布的单播静态路由，可用 **undo ip route-static** *ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* |**tag** *tag*] * **permanent** 命令删除指定的永久发布的静态路由	

10.4.2 配置静态路由与静态 BFD 联动

配置静态路由（可以是静态缺省路由）与静态 BFD 联动，可以快速感知从本地到路由目的地址的链路变化，提高网络可靠性。但在配置静态路由与静态 BFD 联动之前，

需要配置好对应的静态 BFD 会话（有多种静态 BFD 会话，具体配置方法参见第 7 章 7.3 节）。

与 BFD 会话绑定仅可在公网（非特定 VPN 实例网络）静态路由进行配置，配置的方法很简单，仅需在系统视图下执行 **ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] } [**preference** *preference* | **tag** *tag*] * **track bfd-session** *cfg-name* [**description** *text*]命令即可。命令中的参数 **track bfd-session** *cfg-name* 就是要指定用来与所指定的公网静态路由绑定的 BFD 会话名称（所绑定的静态 BFD 会话要事先配置好），为 1～15 个字符，不支持空格。其他参数说明请参见 10.3.1 小节表 1-4 中的第 2 步。但一定要注意：**要确保 BFD 会话和静态路由在同一链路上。**

【示例】将目的地址为 172.16.1.0/16、下一跳 IP 地址为 192.168.1.2/24 的静态路由与名为 atob 的 BFD 会话进行绑定。

```
<Huawei> system-view
[Huawei] ip route-static 172.16.1.0 16 192.168.1.2 track bfd-session atob
```

10.4.3 配置静态路由与 NQA 联动

如果互通设备不支持 BFD 功能，可以配置静态路由与 NQA 联动（在此仅介绍与 NQA ICMP 测试例的联动），利用 NQA 测试例对链路状态进行检测，从而提高网络的可靠性。NQA 把测试两端称为客户端和目的端（或者服务器端），并在客户端发起测试，目的端接收报文后，返回给源端相应的回应信息。根据返回的报文信息，了解相应的网络状况。具体的配置步骤如表 10-5 所示（**第 2～8 步为 NQA 测试例的创建与配置，第 10 步为静态路由与 NQA 测试例的联动**）。

表 10-5　配置静态路由与 NQA 联动的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**nqa test-instance** *admin-name* *test-name* 例如：[Huawei] **nqa test-instance** admin test	创建 NQA 测试例，并进入 NQA 测试例视图。命令中的参数说明如下 • *admin-name*：创建 NQA 测试例的管理员账户，1～32 个字符，不支持空格，区分大小写 • *test-name*：指定 NQA 测试例的测试例名，1～32 个字符，不支持空格，区分大小写 缺省情况下，没能创建任何 NQA 测试例，可用 **undo nqa** { **test-instance** *admin-name test-name* | **all-test-instance** }命令删除指定或所有 NQA 测试例
3	**test-type icmp** 例如：[Huawei-nqa-admin-test] **test-type icmp**	配置测试例类型为 ICMP。静态路由与 NQA 联动时仅采用 ICMP 测试例来检测源端到目的端的路由是否可达 缺省情况下，未配置任何测试类型，可用 **undo test-type** 命令取消对应 NQA 测试例的测试类型配置
4	**destination-address ipv4** *ip-address* 例如：[Huawei-nqa-admin-test] **destination-address ipv4** 1.1.1.1	配置 NQA 测试例的目的 IP 地址（也就是 NQA 测试例的服务器端 IP 地址） 缺省情况下，没有配置目的地址，可用 **undo destination-address** 命令删除 NQA 测试例的目的地址

（续表）

步骤	命令	说明
5	**frequency** *interval* 例如：[Huawei-nqa-admin-test] **frequency** 25	（可选）配置 NQA 测试例的自动执行测试的时间间隔，取值范围为 1～604 800 的整数秒，**必须大于下面第 6 步和第 7 步的取值的乘积** 缺省情况下，没有配置自动测试间隔，即只进行一次测试，可用 **undo frequency** 命令取消 NQA 测试例自动执行测试的时间间隔
6	**interval** { **milliseconds** *interval* | **seconds** *interval* } 例如：[Huawei-nqa-admin-test] **interval seconds** 5	（可选）配置 NQA 测试例的发送报文的时间间隔，命令中的参数说明如下 • **milliseconds** *interval*：二选一参数，以 ms 为单位设置发送报文的时间间隔（当配置的发包间隔的毫秒数是 1 000 的整数倍时，系统会自动把毫秒数转换为秒的形式），取值范围为 10～60 000 ms • **seconds** *interval*：二选一参数，指定以秒设置发送报文的时间间隔，取值范围为 1～60 整数秒 缺省情况下，ICMP 测试类型的发送报文时间间隔为 4 s，可用 **undo interval** 命令恢复 NQA 测试例的发送报文的时间间隔的缺省值
7	**probe-count** *number* 例如：[Huawei-nqa-admin-test] **probe-count** 4	（可选）配置 NQA 测试例一次测试的探针数目，取值范围为 1～15 的整数。通过多次发送 NQA 测试例的测试探针，可以根据统计数据更加准确地评估网络质量 缺省情况下，测试探针数目是 3，可用 **undo probe-count** 命令恢复 NQA 测试例的一次测试探针数目的缺省值
8	**start now** [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second*| *hh:mm:ss* } }] 例如：[Huawei-nqa-admin-test] **start now end at** 08:10:0	（三选一）立即启动测试例 三个命令中的参数说明如下 • **start at** [*yyyy/mm/dd*] *hh:mm:ss*：指定开始执行测试例的时间点，各部分均为整数形式。其中可选参数 *yyyy/mm/dd* 用来指定测试例启动的日期，*yyyy* 指定年，取值范围为 2 000～2 099，*mm* 指定月，取值范围为 1～12，*dd* 指定日，取值范围为 1～31；*hh:mm:ss* 用来指定测试例启动的时刻，*hh* 指定时，取值范围为 0～23；*mm* 指定分钟，取值范围为 0～59；*ss* 指定秒，取值范围为 0～59 • **start delay** { **seconds** *second* | *hh:mm:ss* }：指定延迟启动测试例执行的时间段。其中 **seconds** *second*：指定以秒为单位的延迟启动时间，取值范围为 1～86 399 的整数；*hh:mm:ss* 指定延迟启动的小时、分钟和秒数时间。但以这种方式指定延迟时间后，系统最终会自动转换成以秒表示的形式。比如 1:0:0 表示延迟 1 小时（即 3 600 s）后启动 • **end at** [*yyyy/mm/dd*] *hh:mm:ss*：多选一参数，在指定的时间点结束当前执行的测试例 • **end delay** { **seconds** *second* | *hh:mm:ss* }：多选一参数，指定延迟结束测试例执行的时间。该延迟是相对于当前系统时间的延迟。其中 **seconds** *second* 指定以秒为单位的延迟停止的时间，取值范围为（6～86 399）的整数秒；*hh:mm:ss* 指定延迟指定的时间后停止
	start at [*yyyy/mm/dd*] *hh:mm:ss* [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } |**lifetime** { **seconds** *second* | *hh:mm:ss* } }] 例如：[Huawei-nqa-admin-test] **start at delay** 3600	（三选一）在指定时刻启动测试例

（续表）

步骤	命令	说明
8	**start delay** { **seconds** *second* | *hh:mm:ss* } [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* |*hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] 例如：[Huawei-nqa-admin-test] **start delay lifetime seconds** 600	（三选一）延迟指定时间后启动测试例 ● **end lifetime** { **seconds** *second* | *hh:mm:ss* }：多选一参数，配置测试例的持续时间，以测试例启动时间开始算起。其中 **seconds** *second* 指定以秒为单位设置测试例的生命周期，取值范围为 6～86 399 的整数秒；*hh:mm:ss* 设置测试例的生命周期 缺省情况下，测试报文发送完毕后，测试自动结束，可用 **undo start** 命令终止当前正在执行的测试例或者删除未执行 NQA 测试例的启动方式和结束方式的配置
9	**quit** 例如：[Huawei-nqa-admin-test] **quit**	退出测试例视图，返回系统视图
10	**ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop -address*] } [**preference** *preference* | **tag** *tag*] * **track nqa** *admin-name test-name* [**description** *text*] 例如：[Huawei-nqa-admin-test] **ip route-static** 172.16.2.0 16 **nqa** test	配置静态路由与 NQA 测试例联动。命令中的 **track nqa** *admin-name test-name* 参数用来指定要联动的NQA测试例管理员账户和测试例名称，一定要与本表第 2 步中配置的 NQA 测试例管理员名和测试例名称一致。其他参数请参考 10.3.1 节表 10-4 中的第 2 步 【说明】配置静态路由与 NQA 测试例联动时，不支持 NQA 检测的路由是其所绑定的静态路由的情况；且配置同一条静态路由与其他 NQA 测试例联动时，会解除与前一个 NQA 测试例的联动关系 缺省情况下，没有配置任何静态路由与 NQA 联动，可用 **undo ip route-static** *ip-address* { *mask* | *mask-length* } [*nexthop- address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] * **track nqa** 命令删除指定的静态路由与 NQA 联动

10.4.4　静态路由管理

在完成以上各种静态路由配置后，可以使用 **display** 命令来检查静态路由相关配置，验证配置结果。

① **display ip routing-table**：查看 IPv4 路由表摘要信息。

② **display ip routing-table verbose**：查看 IPv4 路由表详细信息。

③ **display bfd session** all [**verbose**]：查看 BFD 会话信息。

④ **display current-configuration** | **include bfd**：查看静态路由与 BFD 联动的配置。

⑤ **display current-configuration** | **include nqa**：查看静态路由与 NQA 联动的配置。

⑥ **display nqa results** [**collection**] [**test-instance** *admin-name test-name*]：查看 NQA 测试结果。NQA 测试不会在终端自动显示测试结果，必须使用本命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

10.4.5　静态路由配置示例

本示例的基本拓扑结构如图 10-11 所示，3 台路由器连接了 3 台属于不同网段的 PC。现要求通过配置静态路由实现不同网段的任意两台主机之间能够互通。

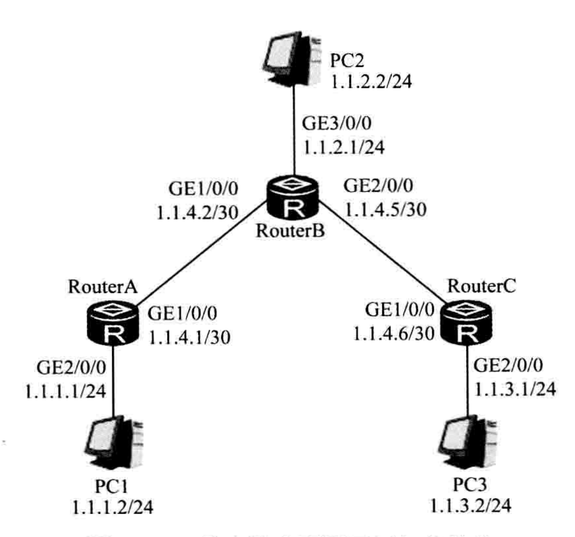


图 10-11　静态路由配置示例拓扑结构

1. 基本配置思路分析

静态路由的配置比较简单，虽然在 10.3.1 小节介绍静态路由命令时看起来参数选项比较多，但实际上在配置静态路由时就是 10.2.1 小节介绍的 5 个主要参数：目的 IP 地址/子网掩码、下一跳 IP 地址、出接口、优先级。

另外，在配置静态路由时一定要注意它的单向性，也就是要使双方能相互访问，必须同时配置往返路径的两条静态路由，也就是通常所说的必须同时有回程路由。当然，还必须在各主机上配置指向连接三层设备 LAN 接口 IP 地址的缺省网关。对于一些单出口的网段，可以利用最简单的缺省路由进行配置，如本示例中 PC1 和 PC3 所在网段。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口 IP 地址配置为例进行介绍，RouterB 和 RouterC 上的接口 IP 地址配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.4.1 30
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 1.1.1.1 24
```

② 配置静态路由。这里可以在 RouterA 和 RouterC 上仅通过配置缺省路由来实现（当然也可以用具体的静态路由），而在 RouterB 上则分别配置到达 PC1 和 PC3 所在网段的两条静态路由。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2          !---配置以 RouterB 的 GE1/0/0 接口 IP 地址作为下一跳的缺省路由
[RouterB] ip route-static 1.1.1.0 255.255.255.0 1.1.4.1    !---配置以 RouterA 的 GE1/0/0 接口 IP 地址作为下一跳，到达 PC1
所在的 1.1.1.0/24 网段的静态路由
[RouterB] ip route-static 1.1.3.0 255.255.255.0 1.1.4.6 !---配置以 RouterC 的 GE1/0/0 接口 IP 地址作为下一跳，到达 PC1
所在的 1.1.3.0/24 网段的静态路由
[RouterC] ip route-static 0.0.0.0 0.0.0.0 1.1.4.5          !---配置以 RouterB 的 GE2/0/0 接口 IP 地址作为下一跳的缺省路由
```

说明 其实在 RouterA 和 RouterC 上也可以采用以下效果更好的，到达 PC2 所在网段的具体静态路由，而不用上面介绍的静态缺省路由。

```
[RouterA] ip route-static 1.1.2.0 255.255.255.0 1.1.4.2
[RouterC] ip route-static 1.1.2.0 255.255.255.0 1.1.4.5
```

③ 配置主机 PC1 的缺省网关为 1.1.1.1，主机 PC2 的缺省网关为 1.2.1.1，主机 PC3 的缺省网关为 1.1.3.1。

配置好后，可以在各路由器上通过执行 **display ip routing-table** 命令查看 IP 路由表，以验证配置结果。下面仅是 RouterA 上的输出示例，从中可以看出，在 IP 路由表中已有一条在前面创建的缺省静态路由（**参见输出信息中的粗体字部分**），其他均为直连路由。其他路由器上的 IP 路由表类似。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11
Destination/Mask    Proto   Pre  Cost   Flags  NextHop      Interface
        0.0.0.0/0   Static  60   0      RD     1.1.4.2      GigabitEthernet1/0/0
       1.1.1.0/24   Direct  0    0      D      1.1.1.1      GigabitEthernet2/0/0
       1.1.1.1/32   Direct  0    0      D      127.0.0.1    GigabitEthernet2/0/0
     1.1.1.255/32   Direct  0    0      D      127.0.0.1    GigabitEthernet2/0/0
       1.1.4.0/30   Direct  0    0      D      1.1.4.1      GigabitEthernet1/0/0
       1.1.4.1/32   Direct  0    0      D      127.0.0.1    GigabitEthernet1/0/0
     1.1.4.255/32   Direct  0    0      D      127.0.0.1    GigabitEthernet1/0/0
      127.0.0.0/8   Direct  0    0      D      127.0.0.1    InLoopBack0
     127.0.0.1/32   Direct  0    0      D      127.0.0.1    InLoopBack0
127.255.255.255/32  Direct  0    0      D      127.0.0.1    InLoopBack0
255.255.255.255/32  Direct  0    0      D      127.0.0.1    InLoopBack0
```

也可以使用 **Ping** 或者 **Tracert** 命令验证各 PC 主机间的连通性，具体示例略。

说明　IP 路由表中"Flags"是路由标记，可以是 R（表示该路由是迭代路由）和 D（表示该路由已下发到 FIB 表）字母，或者它们的组合。但 IP 路由表中的所有路由均有 D 标记，因为它们都下发到了 FIB 中。

10.4.6　静态路由与 BFD 联动配置示例

本示例的基本拓扑结构如图 10-12 所示，RouterA 通过配置静态路由，经由 RouterB 与外部网络相连，其中 RouterA 与 RouterB 之间通过二层交换机 SwitchC 互连。现要求 RouterA 能正常访问外部网络，且要在 RouterA 和 RouterB 之间实现毫秒级故障感知，提高收敛速度。

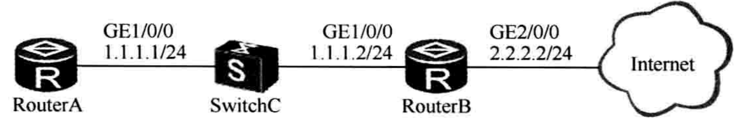


图 10-12　静态路由与 BFD 联动配置示例拓扑结构

1. 基本配置思路分析

本示例要求实现毫秒级的链路故障感知，那么只有通过与 BFD 会话进行绑定了。可以在 RouterA 和 RouterB 上分别创建双向 BFD 会话，并绑定 RouterA 到达外部网络的静

态路由（在这种单一出口网络中可以直接使用静态缺省路由），实现 RouterA 和 RouterB 之间的毫秒级故障感知。

2. 具体配置步骤

① 按照图中标注配置好各路由器接口 IP 地址，下面仅介绍 RouterA 上的接口 IP 地址配置，RouterB 上的配置与 RouterA 上的配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 24
```

② 在 RouterA 上配置与 RouterB 之间的 BFD 会话。

```
<RouterA> system-view
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd aa bind peer-ip 1.1.1.2
[RouterA-bfd-session-aa] discriminator local 10
[RouterA-bfd-session-aa] discriminator remote 20
[RouterA-bfd-session-aa] commit
[RouterA-bfd-session-aa] quit
```

③ 在 RouterB 上配置与 RouterA 之间的 BFD 会话。

```
<RouterB> system-view
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd bb bind peer-ip 1.1.1.1
[RouterB-bfd-session-bb] discriminator local 20
[RouterB-bfd-session-bb] discriminator remote 10
[RouterB-bfd-session-bb] commit
[RouterB-bfd-session-bb] quit
```

④ 在 RouterA 上配置到外部网络的静态缺省路由，并绑定 BFD 会话。

```
[RouterA] ip route-static 0.0.0.0 0 1.1.1.2 track bfd-session aa
```

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all** 命令，可以看到 BFD 会话已经建立，且状态为 Up。在系统视图下执行 **display current-configuration | include bfd** 命令，可以看到静态路由已经绑定 BFD 会话。下面是 RouterA 上的输出显示。

```
[RouterA] display bfd session all
--------------------------------------------------------------------------------
Local  Remote PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
10     20     1.1.1.2         Up        S_IP_PEER   -
--------------------------------------------------------------------------------
       Total UP/DOWN Session Number : 1/0

[RouterA] display current-configuration | include bfd
bfd
bfd aa bind peer-ip 1.1.1.2
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 track bfd-session aa
```

在 RouterA 上执行 **display ip routing-table** 命令，可查看到已配置的静态路由（**参见输出信息中的粗体字部分**）。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 3         Routes : 3
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
```

```
0.0.0.0/0     Static 60   0        RD  1.1.1.2          GigabitEthernet1/0/0
1.1.1.0/24    Direct 0    0         D  1.1.1.1          GigabitEthernet1/0/0
1.1.1.1/32    Direct 0    0         D  127.0.0.1        GigabitEthernet1/0/0
```

对 RouterB 的 GE1/0/0 接口执行 **shutdown** 命令模拟链路故障。然后查看 RouterA 的路由表，发现除了直连路由，静态缺省路由 0.0.0.0/0 也不存在了，如下所示。因为静态缺省路由绑定了 BFD 会话，所以当 BFD 检测到故障后，就会迅速通知所绑定的静态路由不可用。如果未配置静态路由绑定 BFD 会话，静态缺省路由 0.0.0.0/0 不会立即从 IP 路由表删除，可能会造成流量损失。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
          Destinations : 2          Routes : 2
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      1.1.1.0/24    Direct  0    0           D   1.1.1.1         GigabitEthernet1/0/0
      1.1.1.1/32    Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
```

10.4.7　静态路由与 NQA 联动配置示例

如图 10-13 所示，在 RouterB 和 RouterC 上都配置了到用户交换机的静态路由，RouterB 为主用路由器，RouterC 为备用路由器。现要求在正常情况下，SwitchA 上的用户业务流量走主用链路 RouterB→SwitchA，而当主用链路出现故障后，这些用户的业务流量切换到备用链路 RouterC→SwitchA。同样也可配置 SwitchB 上的用户流量主备链路切换。

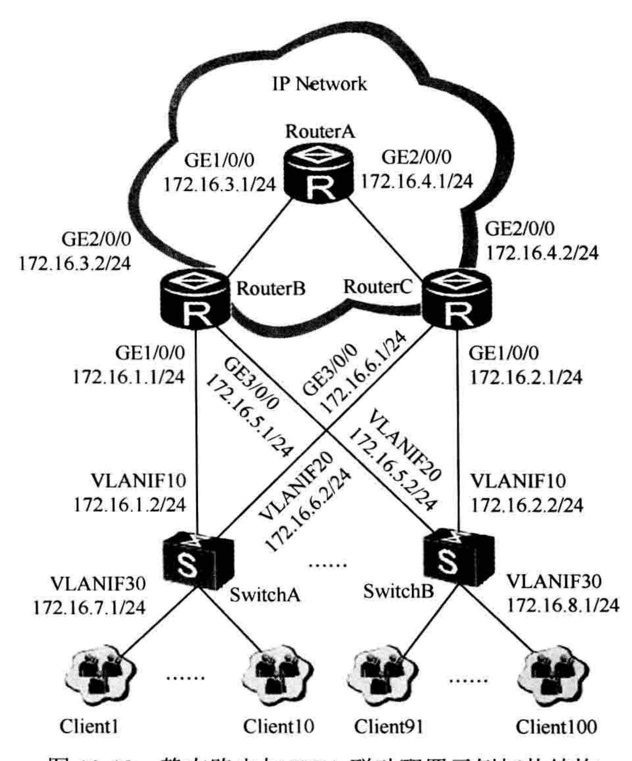


图 10-13　静态路由与 NQA 联动配置示例拓扑结构

1. 基本配置思路分析

本示例是要监控 RouterA 与 SwitchA 之间的链路状态，可以采用静态路由与 NQA 联动的方式进行。具体包括的配置任务如下。

① 在各路由器上配置 IP 地址以及 OSPF 路由协议，并配置不同链路的路由开销值，最终要使得 RouterB 为主用路由器，RouterC 为备用路由器。

② 在 RouterB 与 SwitchA 之间建立 ICMP 类型的 NQA 测试例，同时分别配置 RouterB 和 RouterC 到 SwitchA 上连接的用户网络的静态路由，并且将在 RouterB 配置的静态路由与 NQA 测试例联动，达到快速感知链路故障，实现业务切换的目的。

2. 操作步骤

① 配置各路由器的 IP 地址。现仅以 RouterA 各接口的 IP 地址配置为例进行介绍，其他路由器接口的 IP 地址配置方法与其一样，略。至于各交换机上 VLANIF 接口的配置方法很简单，参见配套图书《华为交换机学习指南》。

```
[RouterA] interface gigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 172.16.3.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitEthernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 172.16.4.1 24
```

② 在 RouterA、RouterB 和 RouterC 上配置 OSPF 动态路由协议，使它们之间三层可达。下面也仅以 RouterA 上的 OSPF 协议配置为例进行介绍，RouterB 和 RouterC 上的配置方法一样，略。此处把它们都放到同一个骨干区域 0 中，仅需要配置基本的接口所连网络的宣告。有关 OSPF 路由协议的详细配置方法参见本书第 12 章。

```
[RouterA] router id 1.1.1.1   !---配置路由器 ID
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] network 172.16.4.0 0.0.0.255
```

③ 为了确保 RouterA 有到达用户网络的路由，需要在 RouterB 和 RouterC 上配置 OSPF 动态路由协议引入静态路由，然后通告给 RouterA。另外，为了使 RouterB 成为主路由器，需要在 RouterB 引入静态路由时开销值更小。

在 RouterB 上配置 OSPF 动态路由协议引入静态路由，并且把路由开销值设置为 10。

```
[RouterB] ospf 1
[RouterB-ospf-1] import-route static cost 10
[RouterB-ospf-1] quit
```

在 RouterC 上配置 OSPF 动态路由协议引入静态路由，并且把路由开销值设置为 20。

```
[RouterC] ospf 1
[RouterC-ospf-1] import-route static cost 20
[RouterC-ospf-1] quit
```

④ 在 RouterB 上配置 RouterB 和 SwitchA 之间的 NQA ICMP 测试例。有关 NAQ ICMP 测试例的配置方法参见第 7 章。

```
<RouterB> system-view
[RouterB] nqa test-instance aa bb
[RouterB-nqa-aa-bb] test-type icmp
[RouterB-nqa-aa-bb] destination-address ipv4 172.16.1.2
[RouterB-nqa-aa-bb] frequency 3
[RouterB-nqa-aa-bb] probe-count 1
```

```
[RouterB-nqa-aa-bb] start now
[RouterB-nqa-aa-bb] quit
```

⑤ 在 RouterB 和 RouterC 上分别配置到达 SwitchA 静态路由（在广播网络中要同时指定出接口和下一跳 IP 地址），但在 RouterB 上配置静态路由时要与配置的 NQA ICMP 测试例进行联动。

```
[RouterB] ip route-static 172.16.7.0 255.255.255.0 gigabitethernet 1/0/0 172.16.1.2 track nqa aa bb

[RouterC] ip route-static 172.16.7.0 255.255.255.0 gigabitethernet 3/0/0 172.16.6.2
```

配置完成后，在 RouterB 的系统视图下执行 **display current-configuration | include nqa** 命令，可以看到静态路由已经绑定 NQA 测试例；执行 **display nqa results** 命令可以看到 NQA 测试例已经建立。如果可以看到"Lost packet ratio: 0 %"，这说明链路状态完好。

```
[RouterB] display current-configuration | include nqa
 ip route-static 172.16.7.0 255.255.255.0 GigabitEthernet1/0/0 172.16.1.2 track nqa aa bb
nqa test-instance aa bb

[RouterB] display nqa results test-instance aa bb
 NQA entry(aa, bb) :testflag is active ,testtype is icmp
  1 . Test 1987 result    The test is finished
   Send operation times: 1                 Receive response times: 1
   Completion:success                       RTD OverThresholds number: 0
   Attempts number:1                        Drop operation number:0
   Disconnect operation number:0           Operation timeout number:0
   System busy operation number:0          Connection fail number:0
   Operation sequence errors number:0     RTT Status errors number:0
   Destination ip address:172.16.1.2
   Min/Max/Average Completion Time: 120/120/120
   Sum/Square-Sum   Completion Time: 120/14400
   Last Good Probe Time: 2012-01-06 19:14:57.5
   Lost packet ratio: 0 %
```

还可通过 **display ip routing-table** 命令查看 RouterB 上的 IP 路由表，从中可以看到静态路由存在于路由表中（**参见输出信息中的粗体字部分**）。

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.1.0/24   Direct  0    0           D   172.16.1.1      GigabitEthernet1/0/0
    172.16.1.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
    172.16.3.0/24   Direct  0    0           D   172.16.3.2      GigabitEthernet2/0/0
    172.16.3.2/32   Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
    172.16.4.0/24   OSPF    10   2           D   172.16.3.1      GigabitEthernet2/0/0
    172.16.5.0/24   Direct  0    0           D   172.16.5.1      GigabitEthernet3/0/0
    172.16.5.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
    172.16.7.0/24   Static  60   0           D   172.16.1.2      GigabitEthernet1/0/0
```

同时可以通过 **display ip routing-table** 命令查看 RouterA 的 IP 路由表。从中可以看到有一条到 172.16.7.0/24 的路由，下一跳指向 172.16.3.2，cost 值为 10，因此业务流量

会优先走链路 RouterB→SwitchA（**参见输出信息中的粗体字部分**）。证明前面在 RouterB 和 RouterC 上配置的到达 SwitchA 的不同静态路由优先级是成功的。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.3.0/24   Direct  0    0           D   172.16.3.1      GigabitEthernet1/0/0
    172.16.3.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.3.2/32   Direct  0    0           D   172.16.3.2      GigabitEthernet1/0/0
    172.16.4.0/24   Direct  0    0           D   172.16.4.1      GigabitEthernet2/0/0
    172.16.4.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.4.2/32   Direct  0    0           D   172.16.4.2      GigabitEthernet2/0/0
    172.16.7.0/24   O_ASE   150  10          D   172.16.3.2      GigabitEthernet1/0/0
```

现在通过 **shutdown** 命令关闭 RouterB 的 GE1/0/0 接口，模拟链路故障。通过 **display nqa results** 命令查看 NQA 测试结果，可以看到“Lost packet ratio: 100 %”（**参见输出信息中的粗体字部分**），这说明链路发生了故障。

```
[RouterB] display nqa results test-instance aa bb
 NQA entry(aa, bb) :testflag is active ,testtype is icmp
  1 . Test 2086 result    The test is finished
   Send operation times: 1                Receive response times: 0
   Completion:failed                        RTD OverThresholds number: 0
   Attempts number:1                         Drop operation number:1
   Disconnect operation number:0           Operation timeout number:0
   System busy operation number:0          Connection fail number:0
   Operation sequence errors number:0     RTT Status errors number:0
   Destination ip address:172.16.1.2
   Min/Max/Average Completion Time: 0/0/0
   Sum/Square-Sum   Completion Time: 0/0
   Last Good Probe Time: 0000-00-00 00:00:00.0
   Lost packet ratio: 100 %
```

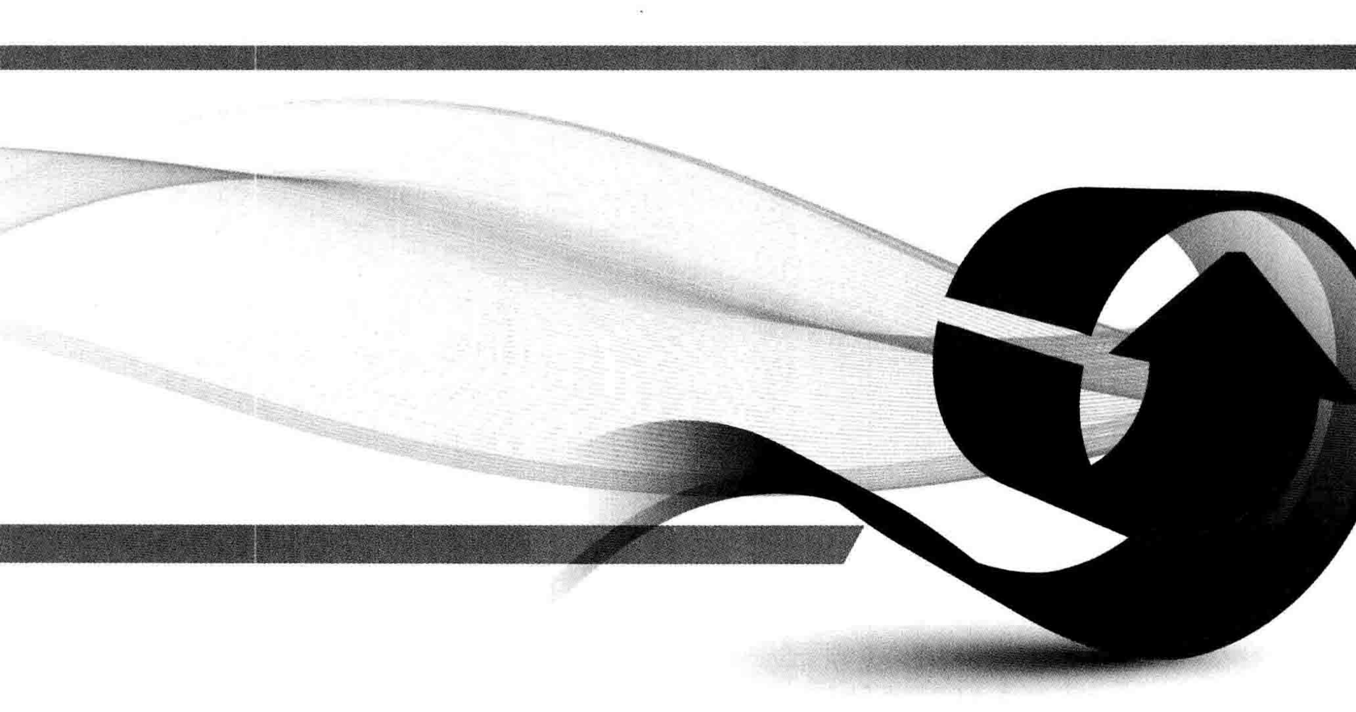
此时再通过 **display ip routing-table** 命令查看 RouterB 上的 IP 路由表，可以看到原来的这条到达 SwitchA 的静态路由消失了，因为 NQA 已通知路由模块对应链路由出现了故障，所以路由模块立即删除了这条静态路由。而在 RouterA 上查看 IP 路由表时，发表到达 SwitchA 的静态路由改为了通过 SwitchC 的静态路由（**参见输出信息中的粗体字部分**）。即通往目的网段 172.16.7.0/24 的路由下一跳指向 172.16.4.2，cost 值为 20，RouterA 仅能从 RouterC 处学到通往 172.16.7.0/24 的路由。由此证明以上的静态路由与 NQA 的联动配置是成功的。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
```

```
  127.0.0.0/8   Direct  0    0        D   127.0.0.1       InLoopBack0
  127.0.0.1/32  Direct  0    0        D   127.0.0.1       InLoopBack0
 172.16.3.0/24  Direct  0    0        D   172.16.3.1      GigabitEthernet1/0/0
 172.16.3.1/32  Direct  0    0        D   127.0.0.1       InLoopBack0
 172.16.3.2/32  Direct  0    0        D   172.16.3.2      GigabitEthernet1/0/0
 172.16.4.0/24  Direct  0    0        D   172.16.4.1      GigabitEthernet2/0/0
 172.16.4.1/32  Direct  0    0        D   127.0.0.1       InLoopBack0
 172.16.4.2/32  Direct  0    0        D   172.16.4.2      GigabitEthernet2/0/0
 172.16.7.0/24  O_ASE   150  20       D   172.16.4.2      GigabitEthernet2/0/0
```

第11章
RIP路由配置与管理



RIP路由是最简单的动态路由协议，主要用于中小型网络。RIP路由的配置也很简单，最基本的配置仅需在各路由器上创建所需的RIP进程，然后宣告各RIP路由器接口直接连接的网段所对应的自然网段就可以把各接口上连接的网段路由向邻居路由器进行通告。除此之外，还可根据实际需要配置RIP路由优先级、开销、3个定时器参数、水平分割、毒性反转、RIPv2的路由聚合、RIPv2报文验证以及RIP路由信息发布和接收控制、RIP与静态BFD/动态BFD联动。

本章将先对RIP路由的主要基础知识（如RIP定时器、RIP报文格式等）和工作原理（如RIP的度量机制、RIP路由更新机制、RIP路由收敛机制等）进行深入分析，然后具体介绍RIP路由各种特性配置与管理方法，同时辅以大量具体配置实例，以加深对这些基础知识、工作原理和功能特性配置的理解。

11.1 RIP 基础

RIP 是一种较为简单的内部网关协议（IGP），包括 RIPv1 和 RIPv2 两个版本。RIPv2 对 RIPv1 进行了扩充，支持 CIDR 和 VLSM 技术，支持安全验证。

由于 RIP 的功能较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，因此 RIP 主要应用于规模较小的网络，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP 协议。

11.1.1 RIP 的度量机制

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，使用跳数（Hop Count）作为度量来衡量到达目的网络的距离。设备到与它直接相连网络的跳数为 0，然后每经过一个三层设备跳数增加 1。也就是说，度量值等于从本网络到达目的网络间的三层设备数量，**但并不是等于所经过的网段数**。

假设在图 11-1 的网络中，4 个路由器都运行了 RIP。现在要配置从 PC1 所在网络到达 PC2 所在网络的 RIP 路由，则跳数就是 3（PC1 直接连接的 R1 不算在内，其他每个路由器算一跳）。但是，这 4 个路由器所连接的网络数达到了 5 个（从 1.1.1.0/24 到 5.1. 1.0/24），所以跳数并不等于所经过的网段数，因为每个路由器还可以连接多个网络。另外要注意的是，在同一个路由器上直接连接的多个网络，彼此间的度量值为 0，因为它们是直连路由。

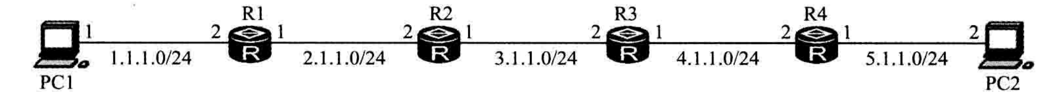


图 11-1　RIP 路由跳数计算示例

RIP 通过 UDP 报文进行路由信息的交换，使用的端口号为 520，所以它又是一个不可靠的路由协议。为限制收敛时间，RIP 规定度量值取 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。也正是由于这个限制，使得 RIP 不可能在大型网络中得到应用。

在定期自动更新过程中，RIP 路由器采用完整路由表更新方式，也就是每个 RIP 路由器会把自己的完整路由表发给相邻的 RIP 路由器，以此来进行彼此的路由表更新。总体来说，它遵循以下几个基本原则。

① 路由表项每经过一次邻居路由器之间的传递，其度量值加 1（最大值为 15，下同）。

在图 11-1 所示的网络中，R1 路由器把它所连接的 1.1.1.0/24 网络向 R2 通告，这时在 R2 上到达 1.1.1.0/24 网络的度量为 1，当 R2 再把它获取的到达 1.1.1.0/24 网络的路由发给 R3 时，R3 上到达 1.1.1.0/24 网络的度量就变为 2，而当 R3 把获取的到达 1.1.1.0/24 网络的路由发给 R4 时，R4 上到达 1.1.1.0/24 网络的度量就变为 3。

② 路由器在收到新的路由更新表项时，会在其路由表中添加新的路由表项，其度量是在接收的路由表项度量基础上加 1，同时在新添加的路由表项中标注其下一跳地址就是发送路由更新的邻居路由器的接口。

在图 11-1 所示的示例中，假设 R4 在收到来自 R3 的路由表更新时发现包含了一条

到达 6.1.1.0/24 网络的新路由表项，并且其度量为 2，这时 R3 就会在自己的路由表中添加这条新的路由表项，并且设置度量为 3（=2+1），“下一跳地址”为 R3 与 R4 相连的那个接口 IP 地址。

③ 收到原有路由表项的路由更新时，先对有更新的路由表项的度量加 1，然后与对应的路由表项中原度量进行比较，**仅接收度量值更小或相等的更新，忽略度量值比原来的值更大的路由更新**。

假设在图 11-1 中，R2 中原有的路由表项如图 11-2 所示，现又收到来自 R3 的如图 11-3 所示的路由更新（启用了水平分割功能后就不会出现这样的更新了，本章后面将具体介绍）。

目的网络	下一跳	距离
2.1.1.0	—	0
3.1.1.0	—	0
4.1.1.0	3.1.1.2	1
5.1.1.0	3.1.1.2	2

图 11-2　R2 路由器上原来的路由表

目的网络	下一跳	距离
2.1.1.0	3.1.1.1	1
3.1.1.0	—	0
4.1.1.0	—	0
5.1.1.0	4.1.1.2	1

图 11-3　R2 收到来自 R3 的路由更新

对于 R2 来说，它在收到来自 R3 的路由更新后，首先对图 11-3 所示的各路由表项的度量加 1，结果得到的路由表项如图 11-4 所示。对比图 11-4 和图 11-2 可以看出，到达 2.1.1.0 网络和 3.1.1.0 网络的度量值比原来的还大，所以忽略更新，而到达 4.1.1.0 网络和 5.1.1.0 网络的度量值是相等的，进行路由表项更新，所以最终 R2 上的路由表还是如图 11-2 所示。

目的网络	下一跳	距离
2.1.1.0	3.1.1.2	2
3.1.1.0	3.1.1.2	1
4.1.1.0	3.1.1.2	1
5.1.1.0	3.1.1.2	2

图 11-4　R2 对收到的路由更新表项度量值加 1 后的路由表

如果一个接口连接的网络没有指定（也就是没有宣告所直接连接的网络），则它不会在任何 RIP 更新中被通告。如图 11-1 所示，在 R1 的配置中没有宣告它所连接的 1.1.1.0/24 网络，则其他路由器上也就没有到达这个网络的 RIP 路由表项，如果这些路由器仅启用了 RIP，且不配置静态路由，则其他路由器也就不能到达 1.1.1.0/24 这个网络了。

当然，到达同一目的网络，也有可能距离是一样的，这时就可能存在同一目的网络的两条 RIP 路由表项。就像多条缺省路由一样，这样两条相同目的网络的 RIP 路由也可以实现负载均衡。

11.1.2　RIP 协议定时器

RIP 在路由更新和维护路由信息时主要使用以下 4 个定时器。

① 更新定时器（Update timer）：当此定时器超时时，立即发送路由更新报文，缺省为每 30 s 发送一次。

② 老化定时器（Age timer）：RIP 设备如果在老化时间内没有收到邻居发来的路由更新报文，则认为该路由不可达。当学到一条路由并添加到 RIP 路由表中时，老化定时

器启动。如果老化定时器超时，设备仍没有收到邻居发来的更新报文，则把该路由的度量值置为 16（表示路由不可达），并启动下面将要介绍的“垃圾收集定时器”。

③ 垃圾收集定时器（Garbage-collect timer）：如果在垃圾收集时间内仍没有收到原来某不可达到路由的更新，则该路由将被从 RIP 路由表中彻底删除。

④ 抑制定时器（Suppress timer）：当 RIP 设备收到对端的路由更新，其度量值为 16，则对应路由进入抑制状态，并启动抑制定时器，缺省为 180 s。这时，为了防止路由振荡，在抑制定时器超时之前，即使再收到对端路由度量值小于 16 的更新，也不接受。当抑制定时器超时后，就重新允许接受对端发送的路由更新报文。

11.1.3 RIP 路由更新机制

RIP 有两种更新机制：一是定期更新，二是触发更新。“定期更新”是根据设置的更新定时器定期发送 RIP 路由通告。该通告报文中携带了除“水平分割”机制抑制的 RIP 路由之外的本地路由器中的**所有 RIP 路由信息**。而“触发更新”则是 RIP 路由器仅在有路由表项发生变化时发送 RIP 路由通告，并**仅携带本地路由表中有变化的路由信息**。RIP 路由器一旦察觉到网络变化，就尽快甚至是立即发送更新报文，而不等待更新周期结束。只要触发更新的速度足够快，就可以极大地防止“计数到无穷大”的发生，但是这一现象还是有可能发生的。

无论是定期更新，还是触发更新，RIP 路由的更新规则如下。

① 如果更新的某路由表项在路由表中没有，则直接在路由表中添加该路由表项。

② 如果路由表中已有相同目的网络的路由表项，且来源端口相同，那么无条件根据最新的路由信息更新其路由表。

③ 如果路由表中已有相同目的网络的路由表项，但来源端口不同，则要比较它们的度量值，将度量值较小的一个作为自己的路由表项。

④ 如果路由表中已有相同目的网络的路由表项，且度量值相等，则保留原来的路由表项。

下面主要介绍 RIP 路由的定期更新机制。

1. RIP 路由定期更新机制

RIP 路由器总是会每隔 30 s（这是缺省值，可以修改，而且也可能与设置值有些偏差）通过 UDP 520 端口以 RIP 广播应答方式向邻居路由器发送一个路由更新包，包中包括了本路由器上的完整的路由表（除了被“水平分割”机制抑制的路由表项），用来向邻居路由器提供路由更新，同时用来向邻居路由器证明自己的存在。RIP 的路由表中主要包括“目的网络”、“下一跳地址”和“距离”这 3 个字段，参见图 11-9。

如果一个路由器在 180 s（这也是缺省值，可以修改）内没有收到某个邻居路由器发来的路由更新，则这个路由器就会标记该邻居路由器为不可达路由器，使这个邻居路由器进入抑制周期。当路由器处于抑制周期内，它仍然可向前转发报文，但网络中的其他路由器不学习到达该路由器所连网络的路由信息，除非是一条更好的到达该路由器所连网络的路由信息，如本来是 3 跳，在抑制周期内学到了一条 2 跳的路由信息。但抑制周期过后，即使是差的路由信息也接受。

如果在连续的 300 s（这也是缺省值，可以修改）内还没收到这个路由器的路由更新，

则本地路由器会在路由表中删除与该邻居路由器相关的路由表项。

由此可见，路由更新不仅影响着整个 RIP 网络中的路由器上路由表的更新和所有需要到达或者经过该路由器的报文路由，还影响着其他邻居路由器对它存在的判定。试想一下，如果有一个报文是要发送到连接某个 RIP 路由器的网络的一台主机上，但这台 RIP 路由器当时恰好出现了故障，此时若没有这个路由器更新机制的话，其他路由器也就不知道它当前出现了故障，会仍按原来的路由路径传输报文，结果当然是报文总是无法到达目的主机了，尽管可能经过了多次尝试。

2. *RIP 路由定期更新机制解析示例*

为了更好地理解 RIP 路由表的更新机制，下面以图 11-5 所示的简单的互连网络为例来讨论图中各个路由器中的路由表是怎样建立的。

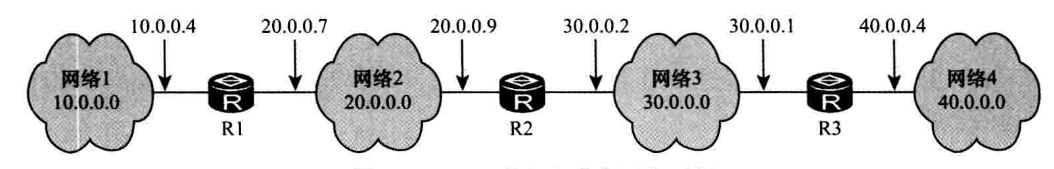


图 11-5　RIP 路由表建立网络示例

① 开始，所有路由器中的路由表只有自己直接连接的网络的路由表项信息。但不是 RIP 路由表项，是直连路由表项，无需下一跳（用“--”表示），度量“距离”也均为 0 ，各路由器的初始路由表如图 11-6 所示，是均只有两条直连网络的路由表项。

R1的路由表

目的网络	下一跳	距离
10.0.0.0	—	0
20.0.0.0	—	0

R2的路由表

目的网络	下一跳	距离
20.0.0.0	—	0
30.0.0.0	—	0

R3的路由表

目的网络	下一跳	距离
30.0.0.0	—	0
40.0.0.0	—	0

图 11-6　R1、R2 和 R3 的初始路由表

② 接下来，各路由器就会按设置的周期（缺省为 30 s）向邻居路由器发送路由更新了。具体哪个路由器会先发送路由更新，取决于哪个路由器先开。现假设路由器 R2 先收到来自路由器 R1 和 R3 的路由更新，并更新了自己的路由表（如图 11-7 所示）。从图中可以看出，它新添加了分别通过 R1 和 R3 到达 10.0.0.0 网络和 30.0.0.0 网络的路由表项，度量值均为 1，因为它只经过了一跳。

③ R2 更新自己的路由表后，会把完整的路由表发给邻居路由器 R1 和 R3。路由器 R1 和 R3 分别再进行更新。根据前面介绍的 RIP 路由表更新的规则可以知道，R1 首先是把从 R2 上接收到的如图 11-7 所示的路由表中的每项度量加 1，得到的路由表如图 11-8 所示。

④ 然后 R1 把图 11-8 所示的路由表与自己原来的路由表（图 11-6 中的左图所示）进行比较，凡是新添加的和度量值小于等于原来的路由表项均将更新，度量值更大的路由表项将忽略更新。经过行比较发现有两条新的路由表项，其目的网络分别为 30.0.0.0 和 40.0.0.0，直接在路由表中添加。而原来已有的两条 10.0.0.0 和 20.0.0.0 表项，发现路由度量（“距离”）值 1 比原来的 0 还大，忽略更新，结果就得到更新后的 R1 路由表，

如图 11-9 所示。

目的网络	下一跳	距离
20.0.0.0	—	0
30.0.0.0	—	0
10.0.0.0	20.0.0.7	1
40.0.0.0	30.1.1.1	1

图 11-7 R2 在路由更新后的路由表

目的网络	下一跳	距离
20.0.0.0	20.0.0.9	1
30.0.0.0	20.0.0.9	1
10.0.0.0	20.0.0.9	2
40.0.0.0	20.0.0.9	2

图 11-8 R1 对收到的来自 R2 路由表进行度量加 1 后形成的路由表

用同样的方法 可以得出 R3 在收到 R2 路由更新后的路由表如图 11-10 所示。但 RIP 路由协议存在一个问题，那就是网络收敛比较慢，当网络出现故障时，要经过比较长的时间才能将此信息传送到所有的路由器，而且中间有许多是无效路由更新。仍以图 11-5 为例，现在 3 个路由器都已经建立了各自的稳定路由表，假设 R1 路由器和网 1（10.0.0.0）的连接线路断开了。

目的网络	下一跳	距离
10.0.0.0	—	0
20.0.0.0	—	0
30.0.0.0	20.0.0.9	1
40.0.0.0	20.0.0.9	2

图 11-9 R1 在收到 R2 路由更新后的路由表

目的网络	下一跳	距离
30.0.0.0	—	0
40.0.0.0	—	0
10.0.0.0	30.0.0.2	2
20.0.0.0	30.0.0.2	1

图 11-10 R3 在收到 R2 路由更新后的路由表

此时 R1 可以立即发现，并更新自己的路由表，将到 10.0.0.0 的路由表项距离改为 16（即不可达），并在 30 s 后将此路由更新信息发给 R2。但是，R2 从 R3 得到的路由更新是“经过 R2 到达 10.0.0.0 网络的距离为 2”，明显度量值更小，于是 R2 将此路由表项更新为“经过 R3 到达 10.0.0.0 的距离为 3”，然后通过路由更新发给 R3，此时 R3 的路由表中更新为“经过 R2 到达 10.0.0.0 网络的距离为 4”。R3 再通过路由更新发给 R2 信息，结果是“经过 R3 到达 10.0.0.0 网络的距离为 5”，一直如此反复，直到该路由表项的距离达到 16，R2 和 R3 才知道 10.0.0.0 网络是不可达的。

为了解决这一不足，出现了水平分割技术，就是同一路由表项更新不再从接收该路由表项的接口发送出去，具体将在本章后面介绍。下面具体介绍 RIP 路由的收敛机制。

11.1.4 RIP 路由收敛机制

任何距离矢量类路由选择协议（RIP 也是这类路由协议）都有一个问题，路由器不知道网络的全局情况，必须依靠相邻路由器来获取网络的可达信息。由于采用 UDP 协议进行的路由更新信息在网络上传播慢，所以所有距离矢量路由算法都有一个收敛慢的问题，这个问题将导致网络中各路由器路由信息不一致的现象产生。RIP 使用以下机制可以减少因网络上的不一致性带来的路由选择环路的可能性。

1. 记数到无穷大机制

RIP 允许最大跳数值为 15。大于 15 的目的地被认为是不可达的。这个数字在限制

了网络大小的同时也防止了一个叫作“记数到无穷大”的问题。记数到无穷大机制的工作原理如图 11-11 所示。

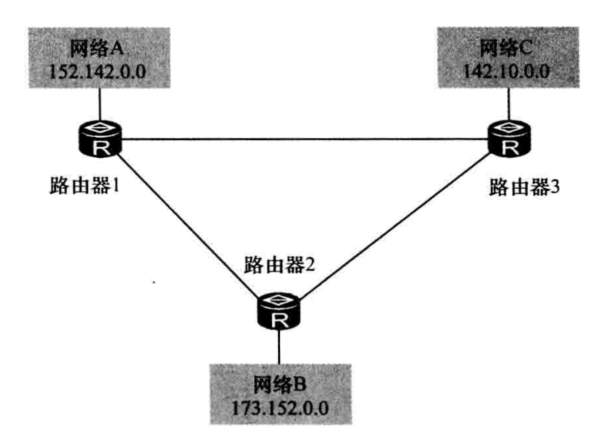


图 11-11　路由器收敛机制示例

① 现假设路由器 1 断开了与网络 A 的连接，此时路由器 1 会立即产生一个路由更新向其邻居路由器 2 和路由器 3 通告，告诉它们，路由器 1 不再有到达网络 A 的路径。假设这个更新信息传输到路由器 2 时被推迟了（CPU 忙、链路拥塞等），但到达了路由器 3，所以路由器 3 会立即从路由表中去掉到网络 A 的路径。

② 但由于路由器 2 没有收到路由器 1 的这个路由更新信息，于是它仍会定期向它的邻居（包括路由器 1 和路由器 3）发送路由更新信息，通告网络 A 是以 2 跳的距离可达。路由器 3 收到这个更新信息后，认为出现了一条通过路由器 2 到达网络 A 的新路径，于是路由器 3 告诉路由器 1，它能以 3 跳的距离到达网络 A。

③ 路由器 1 在收到路由器 3 的路由更新后，把这个信息加上一跳后向路由器 2 和路由器 3 同时发出更新信息，告诉它们路由器 1 可以以 3 跳的距离到达网络 A。

④ 路由器 2 在收到路由器 1 的消息后，比较发现与原来到达网络 A 的路径不符，于是更新成可以以 4 跳的距离到达网络 A。这个消息会再次发往路由器 3，以此循环，直到跳数达到超过 RIP 允许的最大值（在 RIP 中定义为 16）。一旦一个路由器达到这个值，它将声明这条路径不可用，并从路由表中删除此路径。

由于记数到无穷大问题，路由选择信息将从一个路由器传到另一个路由器，每次跳数加 1。路由选择环路问题将无限制地进行下去，除非达到某个限制。这个限制就是 RIP 的最大跳数。当路径的跳数超过 15，这条路径才从路由表中删除。

2. 水平分割法

“水平分割”(Split Horizon)就是使路由器不向对应路由更新表项输入的方向回传此条路由表信息，使它只沿一个方向通告。通俗地讲就是，如果一条路由信息是从某个端口学习到的，那么从该端口发出的路由更新中将不再包含该条路由信息，其目的就是为了避免出现路由更新环路。

水平分割在不同网络中的实现有所区别。在广播网、P2P 和 P2MP 网络中是按照接口进行水平分割的，如图 11-12 所示。

RouterA 会向 RouterB 发送到网络 10.0.0.0/8 的路由信息，如果没有配置水平分割，

RouterB 会将从 RouterA 学习到的这条路由再发送回给 RouterA。这样，RouterA 可以学习到两条到达 10.0.0.0/8 网络的路由：一条为跳数为 0 的直连路由；另一条为下一跳指向 RouterB，跳数为 2 的路由。当 RouterA 到网络 10.0.0.0 的路由变成不可达，并且 RouterB 还没有收到路由不可达的信息时，RouterB 会继续向 RouterA 发送 10.0.0.0/8 可达的路由信息。即 RouterA 会接收到错误的路由信息，认为可以通过 RouterB 到达 10.0.0.0/8 网络；而 RouterB 仍旧认为可以通过 RouterA 到达 10.0.0.0/8 网络，从而形成路由环路。配置水平分割后，RouterB 将不会再把到网络 10.0.0.0/8 的路由发回给 RouterA，由此避免了路由环路的产生。

对于 NBMA（Non-Broadcast Multiple Access）网络，由于一个接口上连接多个邻居，所以是按照邻居进行水平分割的。路由就会按照单播方式发送，同一接口上收到的路由可以按邻居进行区分。从某一接口的对端邻居处学习到路由，不会再通过该接口发送回去。如图 11-13 所示，在 NBMA 网络配置了水平分割之后，RouterA 会将从 RouterB 学习到的 20.0.0.0/8 路由发送给 RouterC，但是不会再发送回给 RouterB。

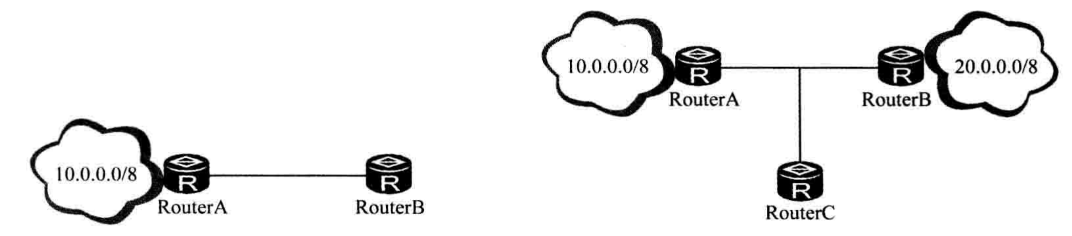


图 11-12 按照接口进行水平分割示意图

图 11-13 按照邻居进行水平分割示意图

3. 毒性反转

“水平分割”功能是路由器用来防止把一个接口得来的路由又从此接口回传，导致路由更新环路的出现。“毒性反转”（Poison Reverse）方法是在更新信息中包括这些回传路由，但会把这些回传路由的跳数直接设为 16（无穷），直接使该路由变为不可达路由（这可能是取“毒性反转”这么看似很严重的名称的原因吧）。通俗地讲就是，如果一条路由信息是从某个端口学习到的，那么从该端口发出的路由更新分组中将继续包含该条路由信息，但将这条信息的 metric 置为 16。通过把跳数设为无穷，并把这条路径告诉源路由器，能够更快地消除路由信息的环路。但它增加了路由更新的负担。

仍以图 11-12 为例进行介绍。配置毒性反转后，RouterB 在接收到从 RouterA 发来的路由后，向 RouterA 发送一个这条路由不可达的消息（将该路由的开销设置为 16），这样 RouterA 就不会再从 RouterB 学到这条可达路由，从而可以避免路由环路的产生。

4. 保持定时器法

“保持定时器法”是设置路由信息被抑制的时间，缺省为 180 s。当路由器接收到一个不可达的路由更新时，路由器会把这条路由更新置于无效抑制状态，不再接收对应路由的更新信息，也不向外发送这条路由更新信息，一直持续到接收到一个带有更好度量的对应路由更新分组，或者这个保持计时器到期为止。

在图 11-11 所示的网络中，由于线路原因，从路由器 1 发往路由器 2 的路由更新被延迟到达，致使路由器 2 不能及时更新，所以路由器 2 仍会以更新后的错误路由信息向路由器 3 发送。但使用了“保持计数器”法后，这种情况将不会发生，因为路由器 3 在收到来自路由

器 1 的网络 A 不可达的路由更新后，将在 180 s 内不接受通向网络 A 的新的路由信息，而经过这段时间后，路由器 2 也已正确进行了更新，将不会再发送错误的路由信息给路由器 3。

11.1.5　RIP 报文格式

目前 RIP 有两种版本，即 RIPv1 和 RIPv2。RIPv1 是有类别路由协议（Classful Routing Protocol），只支持以广播方式发布协议报文。RIPv1 的协议报文中没有携带掩码信息，只能识别 A、B、C 类这样的自然网段的路由（如果连接的是子网，则在进行路由更新通告只能聚合成自然网段的聚合路由向外通告），不支持任意掩码长度的子路由聚合，也不支持不连续子网（Discontiguous Subnet）。RIPv2 是一种无分类路由协议（Classless Routing Protocol）。与 RIPv1 相比，RIPv2 具有以下优势。

① 支持外部路由标记，可以在路由策略中根据 Tag 对路由进行灵活的控制。

② 报文中携带掩码信息，支持任意掩码长度的路由聚合和 CIDR（Classless Inter-Domain Routing，无类别域间路由），即能识别子网路由。

③ 支持指定下一跳，在广播网上可以选择到目的网段的最佳下一跳 IP 地址。

④ 支持以组播方式发送更新报文，减少资源消耗，但只有支持 RIPv2 的设备才能接收这种更新报文。

⑤ 支持对协议报文进行验证，增强安全性。

【经验之谈】所谓“不连续子网”是指在网络中，某几个连续子网在中间被另一个其他网段的子网或网络隔开了。如图 11-14 所示，由 172.16.0.0/16 划分的子网 172.16.1.0/24、172.16.2.0/24 被中间的 192.168.0.0/24 和 192.168.1.0/24 分隔开了，这就是这一个不连续子网。

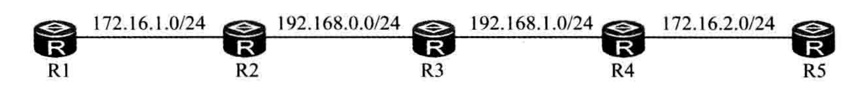


图 11-14　不连续子网示例

图 11-15 所示为一个连续子网，因为在 R3 的左边和右边所连接的子网都不是由一个网络划分的子网，也就是完全不同的子网。

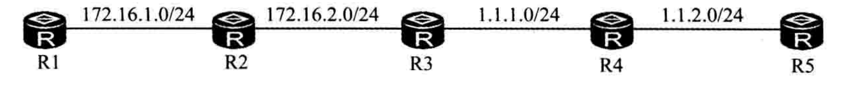


图 11-15　连续子网示例

那么为什么 RIPv1 不支持不连续子网呢？原因就是 RIPv1 路由器接口**在收到不是与接收接口 IP 地址处于同一自然网段的路由更新时会自动进行路由聚合（如果是处于同一自然网段下，则不会聚合，是以具体子网路由显示的）**，而且该自动聚合功能是不可关闭。在如图 11-14 所示的不连续子网中，R3 左边接口在收到 R1 和 R2 连接网段 172.16.1.0/24 的 RIP 路由通告后，由于它与该接口 IP 地址所在网段 192.168.0.0/24 不在同一自动网段下，所以会在 R3 上自动聚合成 172.16.0.0/16 自然网段的聚合路由，其下一跳是 R3 左边接口；同理，R3 右边接口也会对所收到的 R4 和 R5 所连接的 172.16.2.0/24 子网进行自动聚合，且聚合路由也是 172.16.0.0/16 自然网段路由，其下一跳是 R3 右边接口。这时 R3 就不能识别了，因为两边的聚合路由是一样的，但下一跳不一样，这时

在 R3 的 RIP 路由表中会存在两个不同的下一跳，但目的网络均为 172.16.0.0/16 的路由，就会被认为网络中出现了环路。这样的结果就是，在 R3 的左、右边的路由器不能相互学习到所连接的路由，自然也就不能互通了。

如果在图 11-14 中 R2 和 R3 之间连接的是 172.16.3.0/24 网段，则 R3 在收到 R1 和 R2 之间连接网段 172.16.1.0/24 的路由时，在 R3 上就不会被聚合成 172.16.0.0/16，而是以 172.16.1.0/24 的子网路由显示。这时也就不会出现前面所说的环路了，此时图 11-14 当然也不能说成是不连续子网了。

RIP 使用 UDP 报文在邻居路由器间交换路由表，所使用的 UDP 端口号为 520。通常情况下 RIPv1 报文为广播报文；而 RIPv2 报文为组播报文，组播地址为 224.0.0.9，缺省每隔 30 s 向邻居路由器发送一次路由更新报文。如果设备经过 180 s 没有收到来自对端的路由更新报文则将所有来自此设备的路由信息标志为不可达，若在 300 s 内仍未收到更新报文就将这些路由从路由表中删除。图 11-16 所示为 RIP 路由更新报文格式，注意其中 v1 版本和 v2 版本的不同。

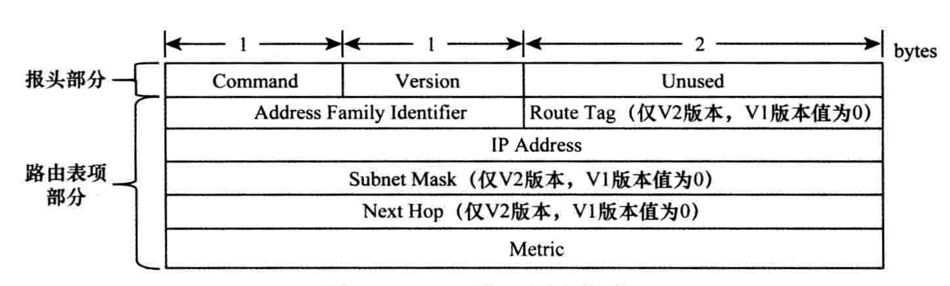


图 11-16 RIP 协议报文格式

（1）Command

命令字段，占 1 个字节，用来指定数据报分组是请求分组，还是响应分组。在 RIPv1 版本中主要有以下 4 种分组类型：Request（请求，对应值为 1）、Response（响应，对应值为 2）、Traceon（启用跟踪标记，对应值为 3，自 RIPv2 版本后已经淘汰）、Traceoff（关闭跟踪标记，对应值为 4，自 RIPv2 版本后已经淘汰）。请求分组是请求邻居路由器发送全部或部分路由表信息的分组，响应分组可以是路由器主动提供的周期性路由更新分组或者是对请求分组的响应。

（2）Version

版本字段，占 1 个字节，RIPv1 版本值为 1，RIPv2 版本值为 2。

（3）Unused

未使用的字段，占 2 个字节，值固定为 0。

（4）Address Family Identifier（AFI）

地址族标识符字段，占 2 个字节，指出所使用的地址族。RIP 设计用于携带多种不同协议的路由信息，每个项都有地址族标志来表明使用的地址类型，IP 地址的 AFI 是 2。

（5）Route Tag

路由标记字段，占 2 个字节，**仅适用于 RIPv2**，RIPv1 版本不适用（值固定为 0）。它提供区分内部路由（由 RIP 学得）和外部路由（由其他协议学得）的方法。它携带着一个 EGP 和 BGP 的自治系统号。因为该字段在 RIPv1 版本中不支持，所以 RIPv1 版本

不支持由其他类型路由重发布为 RIP 路由。

（6）IP Address

IP 地址字段，占 4 个字节，用于指定路由的目的网络地址，可以是标准网段地址、子网地址。

（7）Subnet Mask

子网掩码字段，占 4 个字节，用于指定目的网络的子网掩码，**仅适用于 RIPv2**，RIPv1 版本中该字段的值固定为 0。因为 RIPv1 版本不支持无类别网络，也就是不支持子网路由（但可以连接子网，只是在生成 RIP 路由表项会以有类网络路由显示），仅支持标准的有类网络，所以具体网段的子网掩码是固定的。

（8）Next Hop

下一跳字段，占 4 个字节，**也仅适用于 RIPv2**，RIPv1 版本中该字段的值固定为 0。因为 RIPv1 版本采用的是广播方式发送，无具体的下一跳。它指出 RIP 路由的下一跳的 IP 地址。如果为 0.0.0.0，则表示发布此条路由信息的路由器地址就是最佳下一跳地址。

（9）Metric

RIP 路由的 Metric（度量）值字段，也就是“跳数”值，占 4 个字节，最大有效值为 15。值为 16 时表示该路由不可达。

说明　整 RIP 报文的各字段可分为“头部”（Header）和“路由表项”（Route Entries）两大部分。“头部”包括 Command、Version 和 Unused 这 3 个字段，其余字段都属于“路由表项”。在一个 RIP 报文中，最多可以有 25 个路由表项，也就是在一个 RIP 分组中最多可含有 25 个地址项，即一个分组中最多可一次性通告 25 条 RIP 路由表项。

在 RIP 路由表项部分包括目的 IP 地址/掩码、下一跳 IP 地址、度量，对比 11.2.1 小节介绍的静态路由的组成可以看出前三项是一样的，不同的只是在静态路由中还可以配置出接口，另外在静态路由中的“优先级”其实与 RIP 路由中的“度量”作用差不多，都可体现对应路由的优先级。

11.2　RIP 配置与管理

RIP 的配置任务主要体现在 AR G3 系列路由器对 RIP 特性的支持。AR G3 系列路由器支持的 RIP 特性主要包括 RIP 的基本功能、RIPv2 增强特性、水平分割、毒性反转、控制 RIP 路由的选路、控制 RIP 路由信息的发布和接收、调整 RIP 网络性能参数和 RIP 与 BFD 联动。

下面各小节将分别介绍以上这些 RIP 特性的具体配置方法。

11.2.1　配置 RIP 基本功能

RIP 的基本功能主要包括以下几个方面。

（1）启动 RIP 进程

全局启动 RIP 进程是进行所有 RIP 配置的前提。如果在全局启动 RIP 前，在接口视图下配置了 RIP 相关命令，这些配置只有在全局 RIP 启动后才会生效。

（2）在指定网段使能 RIP

这也就是通常所说的网络宣告。RIP 只在进行网络宣告时所指定网段上的接口才能运行，对于不在指定网段上的接口，RIP 既不在通过它接收和发送路由，也不将它的接口路由转发出去。因此，RIP 启动后必须指定其工作网段。

（3）（可选）配置 NBMA 网络的 RIP 邻居

通常情况下，RIP 使用广播或组播 IP 地址发送报文。**如果在不支持广播或组播报文的 NBMA 网络（如 X.25、ATM 和 FR 等网络）链路上运行 RIP，则必须在链路两端手动相互指定 RIP 的邻居**，这样报文就会以单播形式发送到对端。

（4）（可选）配置 RIP 的版本号

RIP 的版本包括 RIPv1 和 RIPv2 两种，它们的功能有所不同。一般情况下，只需配置全局 RIP 版本号即可。如果需要在指定接口配置与全局不同的 RIP 版本号，则在指定接口下配置接口的 RIP 版本号。

以上 4 项 RIP 基本功能配置任务的具体配置步骤如表 11-1 所示。

表 11-1　　RIP 基本功能的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
启动 RIP 进程	2	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*] 例如：[Huawei] **rip** 10	使能指定的 RIP 进程，进入 RIP 视图（**在一个 RIP 路由器上可以运行多个 RIP 进程**）。命令中的参数说明如下 ● *process-id*：可选参数，指定要使能的 RIP 进程号，取值范围为 1～65 535 的整数。缺省值是 1 ● **vpn-instance** *vpn-instance-name*：可选参数，指定要使能由参数 *process-id* 指定的 RIP 进程的 VPN 实例名，1～31 个字符，不支持空格，**区分大小写**。如果没有指定 VPN 实例，则该 RIP 进程将在公网（非特定 VPN 实例网络）或缺省 VPN 实例下运行 【注意】必须首先全局启动 RIP，才能配置 RIP 的各种全局性参数，但配置与接口相关的 RIP 参数时，不受这个限制，**即可在没有使能 RIP 进程时配置与接口相关的 RIP 参数** 缺省情况下，没有使能 RIP 进程，可用 **undo rip** *process-id* 命令去使能指定的 RIP 进程
	3	**description** *text* 例如：[Huawei-rip-10]**description** this process configure the poison reverse process	（可选）为 RIP 进程配置描述信息，以便识别特定的 RIP 进程、理解不同 RIP 进程的配置。参数 *text* 用来指定 RIP 进程的描述信息，1～80 个字符，支持空格，**区分大小写** 缺省情况下，RIP 进程不附带描述信息，可用 **undo description** 命令删除为对应 RIP 进程配置的描述信息
在指定网段使能 RIP	4	**undo verify-source** 例如：[Huawei-rip-10]**undo verify-source**	（可选）禁止对 RIP 报文的源地址检查 缺省情况下，使能了对收到的 RIP 路由更新报文进行源 IP 地址检查，即检查发送报文的接口 IP 地址与接收报文接口的 IP 地址是否在同一网段。如果不同，则该 RIP 报文将不被设备处理。如果原来已禁止，则可用 **verify-source** 命令使能该功能。**但当 P2P 网络中链路两端的 IP 地址属于不同网络时，只有取消报文的源地址进行检查，链路两端才能建立起正常的邻居关系**

（续表）

配置任务	步骤	命令	说明
在指定网段使能 RIP	5	**network** *network-address* 例如：[Huawei-rip-10]**network** 10.0.0.0	对指定网段接口使能 RIP 路由，即宣告网络。参数 *network-address* 用来指定使能 RIP 的网络地址，**不带子网掩码，因为该地址必须是自然网段的地址，不能是子网地址**。这一点与本书后面将要介绍的 OSPF、IS-S 和 BGP 路由不一样 【注意】如果路由器连接同一自然网段的多个子网，则只需用一条对应自然网段的该命令进行使能 RIP 路由，**也就是一条命令使能了全部同处于该自然网段的接口上的 RIP 路由** 缺省情况下，对指定网段没有使能 RIP 路由，可用 **undo network** *network-address* 命令对指定网段接口去使能 RIP 路由
（可选）配置 NBMA 网络的 RIP 邻居	6	**peer** *ip-address* 例如：[Huawei-rip-10] **peer** 10.0.1.1	（可选）指定 RIP 邻居的 IP 地址，**仅用于 NBMA 网络（如 ATM、X.25 和 FR 网络）中**。配置此命令后，更新报文以单播形式发送到对端，而不采用正常的组播或广播的形式 【说明】通常情况下，不推荐使用该命令，因为这样会造成对端同时收到同一报文的组播（或广播）和单播两种形式。因此建议在配置该命令的同时，使用 **silent-interface** { **all** | *interface-type interface-number* } RIP 视图命令将相关接口改为被动（silent）模式 缺省情况下，系统中没有指定 RIP 邻居的 IP 地址，可用 **undo peer** *ip-address* 命令删除指定的邻居 IP 地址
（可选）配置 RIP 的版本号	7	**version** { **1** | **2** } 例如：[Huawei-rip-10] **version** 2	（可选）指定一个全局 RIP 版本，1 代表 RIPv1 版本，2 代表 RIPv2 版本 缺省情况下，只发送 RIPv1 报文，但可以接收 RIPv1 和 RIPv2 的报文，可用 **undo version** 命令恢复全局 RIP 版本的缺省值
	8	**quit** 例如：[Huawei-rip-10] **quit**	退出 RIP 视图，返回系统视图
	9	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	（可选）键入要配置 RIP 版本的 RIP 路由器接口，进入接口视图
	10	**rip version** { **1** | **2** [**broadcast** | **multicast**] } 例如：[Huawei-GigabitEthernet1/0/0] **rip version** 2 **broadcast**	（可选）配置接口的 RIP 版本。如果配置为 RIPv2 版本，还可选择发送 RIP 协议报文的方式：**broadcast** 为广播方式发送，**multicast** 为组播方式发送 缺省情况下，接口的 RIP 版本配置是继承全局的 RIP 版本配置，即只发送 RIPv1 报文，但可以接收 RIPv1 和 RIPv2 的报文，可用 **undo rip version** 命令恢复缺省配置

说明　当接口中配置的 RIP 版本与全局配置的 RIP 版本不同时，则该接口以本地接口配置的 RIP 版本为准。在接口上配置不同的 RIP 版本，接口允许发送的请求报文和允许接收的响应报文的版本可能会有所不同。

① 如果不配置 RIP 版本，则以广播方式发送 RIPv1 报文，接收广播的 RIPv1 和 RIPv2 报文。

② 如果配置为 RIPv1，则只以广播方式发送 RIPv1 报文，接收广播的 RIPv1 报文。

③ 如果配置为 RIPv2，则只以组播方式发送 RIPv2 报文，接收组播或广播的 RIPv2 报文。

④ 如果配置为组播的 RIPv2（multicast），则以组播方式发送，接收组播 RIPv2 报文。

⑤ 如果配置为广播的 RIPv2(broadcast)，则以广播方式发送 RIPv2 报文，接收 RIPv1 和 RIPv2 的报文。

11.2.2 配置 RIPv2 特性

RIPv2 与 RIPv1 的不同点在于，RIPv2 支持 VLSM（可变长子网掩码）和 CIDR（无类别域间路由），并支持验证功能，从而功能更加完善，安全性更高。

在 RIPv2 特性配置中主要包括以下两方面的配置任务，但它们均不是必须要进行的配置任务，可根据实际需要选择配置。在配置 RIPv2 特性之前，需要配置好上节介绍的 RIP 的基本功能。

1. 配置 RIPv2 的路由聚合

使用路由聚合可以大大减小路由表的规模。另外，通过对路由进行聚合，隐藏一些具体的路由，可以减少路由振荡对网络带来的影响。

RIP 支持两种聚合方式：自动路由聚合和手动路由聚合。**自动路由聚合只能聚合成对应的自然网段，是在系统视图下全局使能的；而手动路由聚合可以是超网路由，是在具体 RIP 路由器接口下配置的。RIPv1 仅支持自动路由聚合，但自动路由聚合功能不可关闭，也就是不可配置**；而 RIPv2 同时支持自动路由聚合和手动路由聚合，且可关闭自动路由聚合功能，以便将子网路由向外发布。自动聚合的路由优先级低于手动指定聚合的路由优先级。

说明 缺省情况下，如果配置了水平分割或毒性反转，有类的自动路由聚合功能将失效。因此在向自然网段边界外发送聚合路由时，相关视图下的水平分割和毒性反转功能都应关闭。

RIPv2 的自动路由聚合和手动路由聚合配置步骤如表 11-2 所示。

表 11-2 RIPv2 的自动路由聚合和手动路由聚合配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei>**system-view**	进入系统视图
方式 1：配置 RIPv2 自动路由聚合		
2	**rip** [*process-id*] 例如：[Huawei]**rip** 10	进入指定的 RIP 视图。如果不指定参数，则直接进入 RIP 进程 1 视图
3	**version 2** 例如：[Huawei-rip-10 **Version 2**	设置 RIP 版本为 RIPv2。只有 RIPv2 的自动路由聚合功能是可配置的，RIPv1 的自动路由聚合功能是不可配置的，总是使能的

（续表）

步骤	命令	说明
4	**summary** [always] 例如：[Huawei-rip-10] **summary**	使能 RIP 有类的自动路由聚合，聚合后的路由以使用自然掩码的路由形式发布。如果选择可选项 **always，则无论水平分割功能是否配置均使能**；如果不选择此可选项，则在配置水平分割或毒性反转的情况下，这种有类聚合功能将失效 缺省情况下，RIP-2 启用有类聚合功能，可用 **undo summary** 命令取消有类聚合以便在子网之间进行路由，此时，子网的路由信息就会被发布出去
方式 2：配置 RIPv2 手动路由聚合		
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置手动路由聚合的 RIP 路由器接口，进入接口视图
3	**rip summary-address** *ip-address mask* [**avoid-feedback**] 例如：[Huawei-GigabitEthernet1/0/0] **rip summary-address 10.0.0.0 255.255.0.0**	配置在以上接口下发布一条 RIP 聚合路由。命令中的参数和选项说明如下 ● *ip-address mask*：指定聚合路由的网络 IP 地址和子网掩码，当然必须与本地接口上所连接的网段对应。可以是对应的自然网段，也可以是超网（**但掩码长度不能小 8 位**） ● **avoid-feedback**：**可选项**，禁止从此接口学习到相同的聚合路由，以免形成路由环路 缺省情况下，系统中没有配置 RIP 路由器发布聚合路由，可用 **undo rip summary-address** *ip-address mask* 命令删除对应的聚合路由

2. 配置 RIPv2 报文的认证方式

在安全性要求较高的网络中，可以通过配置 RIPv2 报文的认证来提高 RIP 网络的安全性。RIPv2 支持对协议报文进行认证，并提供简单认证和 MD5 认证两种方式，增强安全性。其中，简单认证使用未加密的认证字段随报文一同传送，其安全性比 MD5 认证要低。

RIPv2 报文认证需要在具体的 RIP 路由器接口上配置，具体的配置步骤如表 11-3 所示。

表 11-3　RIPv2 报文认证的配置步骤

步骤	命令	说明	
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图	
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置手动路由聚合的 RIP 路由器接口，进入接口视图	
3	**rip authentication-mode simple** { **plain** *plain-text* | [**cipher**] *password-key* } 例如：[Huawei-GigabitEthernet1/0/0]**rip authentication-mode simple plain** huawei	（三选一）配置 RIPv2 报文为简单认证方式	三个命令中的参数和选项说明如下 ● **simple**：指定使用简单认证方式 ● **md5**：指定使用 MD5 密文认证方式 ● **usual**：表示 MD5 密文认证报文使用通用报文格式（IETF 标准） ● **nonstandard**：表示 MD5 密文认证报文使用非标准报文格式

（续表）

步骤	命令	说明	
3	**rip authentication-mode md5 usual** { **plain** *plain-text* | [**cipher**] *password-key* } 或 **rip authentication-mode md5 nonstandard** { **keychain** *keychain-name* | { **plain** *plain-text* | [**cipher**] *password-key*} *key-id* } 例如：[Huawei-GigabitEthernet1/0/0]**rip authentication-mode md5 nonstandard keychain** ripauth	（三选一）配置 RIPv2 报文为 MD5 密文认证方式	• **plain** *plain-text*：**多选一参数**，指定明文认证密码，可以为字母或数字，**区分大小写，不支持空格**。当认证模式为 **simple** 或 **md5 usual** 时，长度为 1～16 个字符；认证模式为 **md5 nonstandard** 或 **hmac-sha256** 时，长度为 1～255 个字符。**但只能键入明文认证密码**，在查看配置文件时以明文方式显示，且密码将以明文形式保存在配置文件中 • [**cipher**] *password-key*：多选一参数，指定密文方式显示的认证密码，可以为字母或数字，**区分大小写，不支持空格**。当认证模式为 **simple** 或 **md5 usual** 时，长度为 1～16 个字符的明文或 24 位和 32 位的密文；认证模式为 **md5 nonstandard** 或 **hmac-sha256** 时，长度为 1～255 个字符的明文或 20～392 位的密文。**可以键入明文或密文认证密码，但在查看配置文件时均以密文方式显示** • **keychain** *keychain-name*：多选一参数，指定使用密钥链表认证方式（**对应的密钥链必须已配置**），密钥链名称为 1～47 个字符，不区分大小写，不支持空格 • *key-id*：指定 MD5 密文认证标识符，取值范围为 1～255 的整数 • **hmac-sha256**：指定使用 HMAC-SHA256 密文认证方式 【说明】密码长度小于等于 16 个字符时，设备上显示以#结尾；密码长度大于 16 个字符时，设备上显示以^#^#开始和结尾 在采用简单认证、MD5 认证方式中，**链路两端所配置的密码必须一致**，否则不能正常建立 UDP 连接，交互 RIP 消息；采用密钥链认证方式以提高 UDP 连接的安全性，**但链路两端必须都配置 Keychain 认证，且配置的 Keychain 必须使用相同的加密算法和密码**，才能正常建立 UDP 连接，交互 RIP 消息 缺省情况下，没有配置认证，可用 **undo rip authentication-mode** 命令取消所有 RIPv2 认证
	rip authentication-mode hmac-sha256 { **plain** *plain-text* | [**cipher**] *password-key* } *key-id* 例如：[Huawei-GigabitEthernet1/0/0] **rip authentication-mode hmac-sha256 plain** huawei	（三选一）配置 RIPv2 报文为 HMAC-SHA256 密文认证方式	

11.2.3 配置防止路由环路

通过配置 RIP 的水平分割和毒性反转特性，可以有效地防止路由环路。水平分割和毒性反转也是在具体的 RIP 路由器接口上配置的，配置也很简单，就是根据需要在对应接口上使能这两种特性，具体配置步骤如表 11-4 所示（**两项配置任务是并列关系，没有先后次序之分**）。在配置 RIP 的水平分割和毒性反转特性之前，也需要完成 RIP 基本功能的配置。

表 11-4　　水平分割和毒性反转特性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置水平分割或毒性反转的 RIP 路由器接口，进入接口视图
3	**rip split-horizon** 例如：[Huawei-GigabitEthernet1/0/0] **rip split-horizon**	（可选）使能 RIP 的水平分割功能。使能了水平分割功能后，从一个接口学习到的路由，当它再从这个接口向外发布时将被禁止 【说明】通常情况下，建议不要取消 RIP 水平分割功能。如果一个接口使能了水平分割并且这个接口还配置了从IP 地址，RIP 更新报文可能不会被每一个从 IP 地址都发送出去，即除非水平分割被禁止，否则一个路由更新不会把每个网络都作为源。如果一个接口与 NBMA 网络连接，那么在缺省情况下，这个接口的水平分割功能将被禁止 如果毒性反转和水平分割都配置了，简单的水平分割行为（从某接口学到的路由再从这个接口发布时将被抑制）会被毒性反转行为代替 缺省情况下，使能 RIP 的水平分割功能，可用 **undo rip split-horizon** 命令去使能 RIP 的水平分割功能
4	**rip poison-reverse** 例如：[Huawei-GigabitEthernet1/0/0] **rip poison-reverse**	（可选）使能 RIP 的毒性反转功能。当配置了毒性反转后，RIP 从某个接口学到路由后，将该路由的开销值设置为 16（不可达），并从原接口发回邻居设备，使邻居设备认为该路由不可达。同时配置水平分割和毒性反转的话，只有毒性反转生效 缺省情况下，没有使能毒性反转功能，可用 **undo rip poison-reverse** 命令去使能 RIP 的毒性反转功能

11.2.4　控制 RIP 的路由选路

通过控制 RIP 的路由选路，使得网络满足复杂环境中的需要。控制 RIP 的路由选路包括的可选配置任务如下（它们是并列关系），可根据实际需要选择配置。在配置 RIP 的路由选路属性之前，也需要先完成 RIP 基本功能的配置。

（1）配置 RIP 协议优先级

当多个路由协议发现目的地相同的路由时，通过配置 RIP 的协议优先级来改变路由协议的优先顺序。

（2）配置接口的附加度量值

对于 RIP 接收和发布路由，可通过调整 RIP 接口的附加度量值来影响路由的选择（**度量值越小越优先**）。附加路由度量值是指在 RIP 路由原来度量值的基础上所增加的度量值（跳数）。

（3）配置最大等价路由条数

通过配置 RIP 最大等价路由条数，可以调整进行负载分担的路由数目。

以上三项配置任务的具体配置步骤如表 11-5 所示（**各项配置任务是并列关系，没有**

先后次序之分）。

表 11-5 控制 RIP 的路由选路的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**rip** [*process-id*] 例如：[Huawei]**rip**	进入对应的 RIP 视图
3	**preference** { *preference* | **route-policy** *route-policy-name* } * 例如：[Huawei-rip-1] **preference** 120 **route-policy** rt-policy1	（可选）配置 RIP 路由的优先级。命令中的参数说明如下： • *preference*：可多选参数，指定路由的优先级，取值范围为 1～255 的整数。缺省值是 100。优先级值越小，优先级越高。如果想让 RIP 路由具有比从其他 IGP 协议学来的路由更高的优先级，需要配置小的优先级值。优先级的高低将最后决定 IP 路由表中的路由采取哪种路由算法获取的最佳路由 • **route-policy** *route-policy-name*：可多选参数，指定路由策略，对满足条件的特定路由设置由参数 *preference* 配置的优先级，1～40 个字符，不支持空格，区分大小写。**有关路由策略的详细介绍和配置方法参见第 15 章** 缺省情况下，RIP 路由的优先级的缺省值为 100，可用 **undo preference** 命令恢复路由优先级的缺省值
4	**maximum load-balancing** *number* 例如：[Huawei-rip-1]**maximum load-balancing** 4	（可选）配置进行负载分担的最大等价路由条数。参数 *number* 用来指定等价路由的数量，AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 的取值范围为 1～4 的整数，AR2220、AR2220L、AR2240/2240-S 和 AR3200 系列的取值范围为 1～8 的整数 缺省情况下，AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2201-48FE/2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 支持最大等价路由的数量是 4，AR2220、AR2220L、AR2240/2240-S 和 AR3200 系列支持最大等价路由的数量是 8，可用 **undo maximum load-balancing** 命令恢复最大等价路由条数的缺省值
5	**quit** 例如：[Huawei-rip-1] **quit**	退出 RIP 视图，返回系统视图
6	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置附加度量值的 RIP 路由器接口，进入接口视图
7	**rip metricin** { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*} *value1*} 例如：[Huawei-GigabitEthernet1/0/0]**rip metricin acl-name** abcd 12	（可选）配置接口接收 RIP 路由更新报文时要给对应路由增加的度量值。命令中的参数说明如下。 • *value*：二选一参数，指定对接收到的路由增加度量值，取值范围为 0～15 的整数。缺省值是 0 • *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*：指定用于接收路由信息过滤的 ACL 表号（**仅支持基本 ACL**），或者 ACL 名称，或者地址前缀列表名，**用于对要接收的 RIP 路由的目的 IP 地址过滤** • *value1*：二选一参数，指定可以通过 ACL 或者 IP 地址前缀列表过滤的度量值，取值范围为 0～15 的整数

（续表）

步骤	命令	说明
7	**rip metricin** { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*} *value1*} 例如：[Huawei-GigabitEthernet1/0/0]**rip metricin acl-name** abcd 12	【说明】在接口上配置好接口在接收 RIP 报文时给路由增加的度量值后，则当该接口接收到一条路由时，RIP 将接口接收权值附加到该路由上，再加入路由表中。所以，增加一个接口的接收 RIP 权值，该接口收到的 RIP 路由权值也会相应增加。通过给接收到的路由增加度量值，可以调整 RIP 的选路 缺省情况下，接口接收 RIP 报文时不给路由增加度量值，可用 **undo rip metricin** 命令恢复该附加度量值的缺省值
8	**rip metricout** { *value* | { *acl-number* | acl-name *acl-name* | **ip-prefix** *ip-prefix-name*} *value1*} 例如：[Huawei-GigabitEthernet1/0/0]**rip metricout ip-prefix** p1 12	（可选）配置接口发送 RIP 路由更新报文时要给对应路由增加的度量值。命令中的参数说明参见上一步中对应的参数，只不过这里是对接口发送的 RIP 路由报文所增加的附加度量值 缺省情况下，接口发送 RIP 报文时给路由增加度量值为 1，可用 **undo rip metricout** 命令恢复该度量值为缺省值 【说明】当发布一条路由时，发送度量值会在发布该路由之前附加在这条路由上。因此，增加一个接口的发送度量值后，该接口发送的 RIP 路由权值也会相应增加。但本地路由表中的度量值不会发生改变 当用 ACL 或 ip-prefix 方式设置接口发送 RIP 路由增加的度量值时，指定 *value1* 为通过过滤策略的 RIP 路由增加相应的度量值，而没有通过过滤的 RIP 路由增加的度量值仍为缺省的 1 对于命名型 ACL，使用 **rule** 命令配置过滤规则时，只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对过滤规则有效

【示例 1】设置 RIP 接收路由的附加度量值为 12。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricin 12
```

【示例 2】对通过名称为“abcd”的 ACL 过滤的路由设置增加度量值 12。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricin acl-name abcd 12
```

【示例 3】对通过 IP 地址前缀列表“ip1”过滤的路由设置增加度量值 12。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricin  ip-prefix ip1 12
```

【示例 4】设置 RIP 发送度量值为 12。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricout 12
```

【示例 5】设置用编号为 2050 的 ACL 过滤的 RIP 路由的发送度量值为 12。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricout 2050 12
```

【示例 6】设置用 IP 地址前缀列表 p1 过滤的 RIP 路由的发送度量值为 12。

```
<Huawei> system-view
[Huawei] ip ip-prefix p1 permit 10.10.10.1 24
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricout ip-prefix p1 12
```

11.2.5 控制 RIP 路由信息的发布

对 RIP 路由信息的发布进行精确的控制，可以满足复杂网络环境中的需要。具体操作时主要包括以下可选配置任务（它们的配置是并列关系），可根据实际需要选择配置。同样，在控制 RIP 路由信息的发布之前，需要配置 RIP 的基本功能。

（1）配置 RIP 发布缺省路由

在路由表中，缺省路由以到网络 0.0.0.0（掩码也为 0.0.0.0，代表任意网络）的路由形式出现。当报文的目的地址不能与路由表的任何目的地址匹配时，设备将选取缺省路由转发该报文。

（2）配置 RIP 引入外部路由信息

RIP 可以引入其他进程或其他协议学习到的路由信息，从而实现与其他协议的网络互通。

（3）禁止接口发送更新报文

通过配置禁止接口发送更新报文，可以防止路由环路。禁止接口发送更新报文有两种实现方式：一是在 RIP 进程下全局配置接口为抑制状态；二是在接口视图下禁止具体接口发送 RIP 报文。在 RIP 进程下的全局配置的优先级要高于在接口视图下的配置。

以上三项配置任务的具体配置步骤如表 11-6 所示（**各项配置任务是并列关系，没有先后次序之分**）。

表 11-6 控制 RIP 路由信息发布的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**rip** [*process-id*] 例如：[Huawei]**rip**	进入对应的 RIP 视图
配置 RIP 发布缺省路由	3	**default-route originate** [**cost** *cost* | { { **match default** | **route-policy** *route-policy-name* } [**avoid-learning**] }]* 例如：[Huawei-rip-1] **default-route originate cost** 2	（可选）配置当前设备生成一条缺省路由或者将路由表中存在的缺省路由发送给邻居路由器。命令中的参数和选项说明如下 • **cost** *cost*：可多选参数，指定生成的缺省路由的度量值，取值范围为 0～15 的整数，缺省值是 0 • **match default**：二选一选项，指定当在路由表中存在其他路由协议或其他 RIP 进程生成的缺省路由时，则向邻居发布该缺省路由 • **route-policy** *route-policy-name*：二选一参数，指定生成缺省路由策略名称，1～40 个字符，区分大小写，不支持空格 • **avoid-learning**：可选项，指定当路由表中已有活跃的缺省路由时，则不引入其他缺省路由 配置本命令后，只有在路由表中有缺省路由时才能向 RIP 邻居发送缺省路由，并且之前从邻居学习到的缺省路由将被删除 缺省情况下，当前设备不向邻居发送缺省路由，可用 **undo default-route originate** 命令恢复缺省情况

（续表）

<table>
<tr><th>配置任务</th><th>步骤</th><th>命令</th><th>说明</th></tr>
<tr><td rowspan="3">配置 RIP 引入外部路由信息</td><td>4</td><td>default-cost cost
例如：[Huawei-rip-1] default-cost 2</td><td>（可选）配置引入路由的缺省开销值，取值范围为 0～15 的整数，缺省值为 0。引入后，最终的开销值还将增加 1
缺省情况下，引入路由的缺省开销值为 0，可用 undo default-cost 命令恢复引入路由的缺省开销值为缺省值</td></tr>
<tr><td>5</td><td>import-route bgp [permit-ibgp] [cost { cost | transparent } | route-policy route-policy-name] *
或
import-route { {static | direct | unr} | { { rip | ospf | isis } [process-id] } } [cost cost | route-policy route-policy-name] *
例如：[Huawei-rip-1] import-route isis 7 cost 7</td><td>引入外部路由信息，包括静态路由、直连路由、BGP/OSPF/IS-IS 路由，以及其他进程的 RIP 路由。两个命令中的参数和选项说明如下
• bgp | static | direct | rip | ospf | isis| unr：多选一选项，指定要引入 BGP 路由、静态路由、直连路由、RIP 路由、OSPF 路由、IS-IS 路由和用户网络端主机上的路由
• permit-ibgp：可选项，指定公网实例下的 RIP 进程可以引入 IBGP 路由
• process-id：可选参数，指定要进入的路由的进程号，取值范围为 1～65 535 的整数，仅适用于 RIP、OSPF、IS-IS 路由
• cost cost：二选一参数，指定引入路由的开销值，取值范围为 0～15 的整数
• cost transparent：二选一选项，指定引入路由的开销值为 BGP 路由的 MED（多出口区分）特性值
• route-policy route-policy-name：可多选参数，指定用于过滤路由信息引入的路由策略名称，1～40 个字符，不支持空格，区分大小写
缺省情况下，不从其他路由协议引入路由，可用 undo import-route { { static | direct | bgp | unr } | { { rip | ospf | isis } [process-id] } }命令取消从对应的外部路由协议中引入路由</td></tr>
<tr><td>6</td><td>filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export [protocol [process-id] |interface-type interface-number]
例如：[Huawei-rip-1] filter-policy 2002 export isis 1</td><td>（可选）在向外发布路由更新时对引入的路由信息进行过滤。命令中的参数说明如下
• acl-number | acl-name acl-name | ip-prefix ip-prefix-name：指定用于路由信息发布过滤的 ACL 表号，或者 ACL 名称，或者地址前缀列表名，用于对要发布的外部路由的目的 IP 地址过滤
• protocol：二选一参数，指定要过滤向外发布的引入路由信息的协议类型，可以是 static、direct、rip、ospf、isis、bgp 和 unr
• process-id：可选参数，指定要过滤向外发布的引入路由信息所对应的路由进程号，取值范围为 1～65 535 的整数，当参数 protocol 取值为 isis、rip 和 ospf 时必须同时指定进程号
• interface-typeinterface-number：二选一参数，指定要过滤向外发布的引入路由信息所对应的出接口（也就是引入该外部路由的接口）
缺省情况下，系统中没有配置该过滤策略，可用 undo filter-policy [acl-number | acl-name acl-name | ip-prefix ip-prefix-name] export [protocol [process-id] | interface-type interface-number]命令删除指定的引入路由信息向外发布的过滤策略</td></tr>
</table>

（续表）

配置任务	步骤	命令	说明
禁止接口发送更新报文	7	**silent-interface** { **all**| *interface-type interface-number* } 例如：[Huawei-rip-100] **silent-interface** gigabitethernet 1/0/0	（可选）抑制所有（选择 all 选项时）或者指定（选择 *interface-type interface-number* 参数时）RIP 路由器接口，使其只接收报文，用来更新自己的路由表，而不发送 RIP 报文 缺省情况下，不使能该抑制功能，可用 **undo silent-interface** { **all** | *interface-type interface-number* } 命令使能所有或者指定 RIP 路由器接口发送更新报文 【说明】该命令可与 **peer** *ip-address* 命令协同使用，使抑制的接口仍可向指定的邻居路由器发布路由
	8	**quit** 例如：[Huawei-rip-1] **quit**	退出 RIP 视图，返回系统视图
	9	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要禁止发送 RIP 报文的 RIP 路由器接口，进入接口视图
	10	**undo rip output** 例如：[Huawei-GigabitEthernet1/0/0] **undo rip output**	（可选）禁止以上接口发送 RIP 报文 缺省情况下，允许接口发送 RIP 报文，可用 **rip output** 命令允许接口发送 RIP 报文。但第 7 步的配置优先级高于本步

【示例 1】设置路由表中存在的缺省路由的度量值为 2。

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate match default cost 2
```

【示例 2】设置路由器基于符合路由策略名称为 filter 的路由生成一条缺省路由，并设置其 cost 值为 15。

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate route-policy filter cost 15
```

【示例 3】避免引入其他路由协议或其他 RIP 进程的缺省路由。

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate match default avoid-learning
```

【示例 4】按照地址前缀列表 abc，对引入的静态路由过滤，通过过滤的路由加入 RIP 路由表，并作为 RIP 路由更新报文发送出去。

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] filter-policy ip-prefix abc export static
```

【示例 5】按照 ACL 2002，对引入的 IS-IS 进程 1 路由过滤，通过过滤的路由加入 RIP 路由表，并作为 RIP 路由更新报文发送出去。

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] filter-policy 2002 export isis 1
```

【示例 6】配置 RIP 接口 GE1/0/0 为抑制状态，但仍可以向 IP 地址为 10.1.1.1/24 的网段邻居发送 RIP 路由更新报文。

```
<Huawei> system-view
[Huawei] rip 100
```

```
[Huawei-rip-100] silent-interface gigabitethernet 1/0/0
[Huawei-rip-100] peer 10.1.1.1
```

11.2.6　控制 RIP 路由信息的接收

对 RIP 路由信息的接收进行精确的控制，可以满足复杂网络环境中的需要。要实现控制，主要要进行以下配置任务，它们的配置是并列关系，可根据实际需要选择配置。同样，在控制 RIP 路由信息的接收之前，需要配置 RIP 的基本功能。

（1）禁止 RIP 接收主机路由

在某些特殊情况下，路由器会收到大量来自同一网段的 RIP 的 32 位主机路由，这些路由对于路由寻址没有多少作用，却占用了大量网络资源。

（2）配置 RIP 对接收的路由进行过滤

通过指定访问控制列表和地址前缀列表，可以配置入口过滤策略，对接收的路由进行过滤，使只有通过过滤的路由才能被加入本地路由表中。

（3）禁止接口接收更新报文

通过配置禁止接口接收更新报文，可以防止路由环路。

以上 3 项配置任务的具体配置步骤如表 11-7 所示（**各项配置任务是并列关系，没有先后次序之分**）。

表 11-7　控制 RIP 路由信息接收的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
	2	**rip** [*process-id*] 例如：[Huawei]**rip**	进入对应的 RIP 视图
禁止 RIP 接收主机路由	3	**undo host-route** 例如：[Huawei-rip-1] **undo host-route**	禁止 32 位主机路由加入 RIP 路由表 缺省情况下，允许主机路由加入 RIP 路由表里，可用 **host-route** 命令允许 32 位主机路由加入 RIP 路由表
配置 RIP 对接收的路由进行过滤	4	**filter-policy** { *acl-number* | **acl-name** *acl-name* } **import** [*interface-type interface-number*] 例如：[Huawei-rip-1] **filter-policy** 2002 **import** gigabitethernet 1/0/0	（三选一）配置基于 ACL 过滤学到的路由信息。命令中的参数说明如下 • *acl-number* | **acl-name** *acl-name*：指定用于过滤学到的路由信息的 ACL 列表号（取值范围为 2 000～2 999 的整数，即仅可是基本 ACL）或列表名称 • *interface-type interface-number*：指定基于入接口过滤学到的路由信息的接口。如果不指定此可选参数，则所有符合 ACL 规则的路由都将接收 缺省情况下，系统中没有配置该过滤策略，可用 **undo filter-policy** [*acl-number* | **acl-name** *acl-name*] **import** [*interface-type interface-number*] 命令用来删除指定的过滤策略
		filter-policy gateway *ip-prefix-name* **import** 例如：[Huawei-rip-1] **filter-policy gateway** abc **import**	（三选一）配置基于发布网关（也就是发布对应流入路由的网关）过滤邻居发布的路由信息。命令中的 *ip-prefix-name* 参数用来指定用于过滤学到的路由信息所对应的发布网关的地址前缀列表名称 缺省情况下，系统中没有配置该过滤策略，可用 **undo filter-policy gateway** *ip-prefix-name* **import** 命令删除指定的过滤策略

（续表）

配置任务	步骤	命令	说明
配置 RIP 对接收的路由进行过滤	4	**filter-policy ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] **import** [*interface-type interface-number*] 例如：[Huawei-rip-1] **filter-policy ip-prefix** abc **gateway** wgprefix **import**	（三选一）配置对指定接口学到的路由进行基于目的地址前缀和基于邻居的过滤。命令中的参数说明如下 ● *ip-prefix-name*：指定用于过滤路由信息目的地址的地址前缀列表名 ● **gateway** *ip-prefix-name*：可选参数，指定用于过滤路由信息目的地址所对应的发布网关的地址前缀列表名 ● *interface-type interface-number*：可选参数，指定基于入接口过滤学到的路由信息的接口。如果不指定此可选参数，则所有符合地址前缀列表条件，或者同时符合网关地址前缀列表条件的路由都将接收 缺省情况下，系统中没有配置该过滤策略，可用 **undo filter-policy ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] **import** [*interface-type interface-number*]命令删除指定的过滤策略
禁止接口接收更新报文	5	**quit** 例如：[Huawei-rip-1] **quit**	退出 RIP 视图，返回系统视图
	6	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要禁止发送 RIP 报文的 RIP 路由器接口，进入接口视图
	7	**undo rip input** 例如：[Huawei-GigabitEthernet1/0/0] **undo rip output**	（可选）禁止以上接口接收 RIP 报文 缺省情况下，允许接口接收 RIP 报文，可用 **rip input** 命令允许接口接收 RIP 报文，但第 7 步的配置优先级高于本步

11.2.7 调整 RIP 网络性能参数

在某些特殊的网络环境中可能需要重新调整一些 RIP 参数，如 RIP 定时器、报文的发送间隔、最大数量等，以便提升 RIP 网络的性能，主要包括以下配置任务，它们的配置是并列关系，可根据实际需要选择配置。同样，在调整 RIP 性能参数之前，需要配置 RIP 的基本功能。

（1）配置 RIP 定时器

RIP 有 3 个定时器：Update、Age 和 Garbage-collect。改变这几个定时器的值，可以影响 RIP 的收敛速度。有关这 3 个定时器的说明参见 11.1.2 小节。

（2）配置 RIP 对更新报文进行有效性检查

通过 RIP 对更新报文进行有效性检查，可以提高网络安全性。该有效性检查包括 RIPv1 报文的零域检查和 RIP 更新报文的源地址检查两种。

① RIPv1 报文中的有些字段必须为零，称为零域（参见 11.1.5 小节的图 11-16）。RIPv1 在接收报文时将对零域进行检查，若 RIPv1 报文中零域的值不为零，该报文将不被处理。

② RIP 在接收报文时将对源 IP 地址进行检查，即检查发送报文的接口 IP 地址与接收报文接口的 IP 地址是否在同一网段。如果没有通过检查，则该 RIP 报文将不被路由器处理。

（3）配置报文的发送间隔和发送报文的最大数量

通过设置 RIP 发送更新报文的时间间隔和每次发送报文的最大数量，可以很好地控制路由器用于处理 RIP 更新报文的内存资源。

（4）使能 Replay-protect 功能

通过使能 Replay-protect（重放保护）功能，可以得到接口 Down 之前所发送 RIP 报文的 Identification（标识符），避免双方的 RIP 路由信息不同步、丢失。

假设运行 RIP 的接口状态变为 Down 之前发送的最后的 RIP 报文的 Identification 为 *X*，该接口状态变为 Up 后，再次发送 RIP 报文的 Identification 会变为 0。如果对方没有收到这个 Identification 为 0 的 RIP 报文，那么后续的 RIP 报文都将被丢弃，直到收到 Identification 为 *X*+1 的 RIP 报文。这样就会导致双方的 RIP 路由信息不同步、丢失。通过使能 Replay-protect 功能，当接口从 Down 变为 Up 之后，再次发送 RIP 报文的 Identification 会顺次加 1，从而避免了上述情况的发生。

以上 4 项配置任务的具体配置步骤如表 11-8 所示。（**各项配置任务是并列关系，没有先后次序之分**）。

表 11-8　　调整 RIP 网络性能参数的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**rip** [*process-id*] 例如：[Huawei]**rip**	进入对应的 RIP 视图
配置 RIP 定时器	3	**timers rip** *update age garbage-collect* 例如：[Huawei-rip-1] **timers rip** 35 170 240	调整 RIP 定时器。命令中的参数说明如下 ● *update*：指定路由更新报文的发送间隔，取值范围为 1～86 400 的整数秒 ● *age*：指定 RIP 路由的老化时间，取值范围为 1～86 400 的整数秒 ● *garbage-collect*：指定路由被从路由表中删除的时间，取值范围为 1～86 400 的整数秒 以上三个定时器参数的取值要遵循以下关系：*update*<*age*，*update*<*garbage-collect*
配置 RIP 对更新报文进行有效性检查	4	**checkzero** 例如：[Huawei-rip-1] **checkzero**	（三选一）使能对 RIPv1 报文中的零域进行检查 【说明】RIPv1 报文中的有些字段必须为零，称为零域，本命令仅适用于 RIPv1 报文。RIPv1 在接收报文时将对零域进行检查，零域的值不为零的 RIP-1 报文将不被处理 缺省情况下，已使能对 RIPv1 报文的零域检查功能，可用 **undo checkzero** 命令去使能该功能
	5	**verify-source** 例如：[Huawei-rip-1] **verify-source**	使能对收到的 RIP 路由更新报文进行源 IP 地址检查，即检查发送报文的接口 IP 地址与接收报文接口的 IP 地址是否在同一网段。如果不在同一网段，则该 RIP 报文将不被设备处理 缺省情况下，已使能对收到的 RIP 路由更新报文进行源 IP 地址检查，可用 **undo verify-source** 命令去使能该功能

（续表）

配置任务	步骤	命令	说明
配置报文的发送间隔和发送报文的最大数量	6	**quit** 例如：[Huawei-rip-1] **quit**	退出 RIP 视图，返回系统视图
	7	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置 RIP 报文的发送时间间隔和发送报文的最大数量，或者配置重放保护功能的 RIP 路由器接口，进入接口视图
	8	**rip pkt-transmit** { **interval** *interval* | **number** *pkt-count* } * 例如：[Huawei-GigabitEthernet1/0/0] **rip pkt-transmit interval** 60 **number** 100	在以上接口上设置 RIP 发送更新报文的时间间隔和每次发送报文的数量。命令中的参数说明如下 • **interval** *interval*：可多选参数，指定 RIP 路由更新报文发送的时间间隔，取值范围为 50～500 的整数秒 • **number** *pkt-count*：可多选参数，指定队列中每次发送的 RIP 路由更新报文的数量，取值范围为 25～100 的整数 缺省情况下，RIP 接口发送 RIP 路由更新报文的时间间隔为 200 ms，每次发送的 RIP 路由更新报文数量为 50，可用 **undo rip pkt-transmit** 命令恢复接口上其缺省值
使能 Replay-protect 功能	9	**rip authentication-mode md5 nonstandard** *password-key key-id* 例如：[Huawei-GigabitEthernet1/0/0] **rip authentication-mode md5 nonstandard** hawei 1	配置 RIP-2 使用 MD5 密文的验证方式，验证报文使用非标准报文格式。命令中的参数说明如下 • *password-key*：指定密文方式显示的验证密码，可以为字母或数字，1～255 个字符的明文或 20～392 位的密文密码，**区分大小写**，不支持空格 • *key-id*：指定 MD5 密文验证标识符，取值范围为 1～255 的整数 缺省情况下，没有配置验证，可用 **undo rip authentication-mode** 命令取消所有验证
	10	**rip replay-protect** 例如：[Huawei-GigabitEthernet1/0/0] **rip replay-protect**	在以上接口上使能 replay-protect 功能 缺省情况下，不使能 replay-protect 功能，可用 **undo rip replay-protect** 命令去使能该功能

11.2.8 配置 RIP 与 BFD 联动

通常情况下，RIP 通过定时接收和发送路由更新报文来保持邻居关系，若在老化定时器设定的时间内没有收到邻居发送的更新报文，则宣告邻居状态变为 Down。因为老化定时器的缺省值为 180 s，所以在链路出现故障时，RIP 至少要经过 180 s 才会检测到。这时，如果网络中部署了高速数据业务，在此期间将导致数据大量丢失。BFD 能够提供毫秒级别的故障检测机制，可以及时检测到被保护的链路或节点故障，并上报给 RIP，而实现 RIP 路由的快速收敛。

当网络中运行高速率数据业务时，可以通过配置 BFD 与 RIP 联动实现 RIP 对网络中的故障快速作出响应的目的。可以配置 RIP 与静态或者动态 BFD 联动（它们是并列关系），并可根据实际需要选择配置。但在配置 RIP 与 BFD 联动之前，也需要完成 RIP 基本功能的配置。有关 BFD 的详细介绍参见第 7 章。

如图 11-17 所示，RouterA、RouterB、RouterC 及 RouterD 建立 RIP 邻接。经过路由计算，RouterA 到达 RouterD 的路由下一跳为 RouterB。在 RouterA 及 RouterB 上使能

RIP 与动态 BFD 联动检测机制。

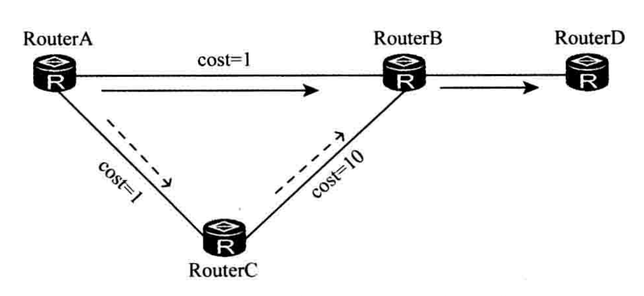


图 11-17　RIP 路由与 BFD 联动示例

当 RouterA 和 RouterB 之间的链路出现故障时，BFD 快速感知并通知给 RouterA，RouterA 删除下一跳为 RouterB 的路由。然后 RouterA 重新进行路由计算并选取新的路径，新的路由经过 RouterC、RouterB 到达 RouterD。当 RouterA 与 RouterB 之间的链路恢复之后，二者之间的会话重新建立，RouterA 收到 RouterB 的路由信息，重新选择最优路径进行报文转发。

1. 配置 RIP 与动态 BFD 联动

配置 RIP 与动态 BFD 联动有两种方式。

① RIP 进程下全局使能 BFD。当网络中大部分 RIP 接口需要使能 RIP 与动态 BFD 联动时，建议选择此方式。

② RIP 接口下使能 BFD。当网络中只有小部分 RIP 接口需要使能 RIP 与动态 BFD 联动时，建议选择此方式。

以上两种方式的具体配置步骤如表 11-9 所示。

表 11-9　RIP 与动态 BFD 联动的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 全局视图
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
方式 1：在 RIP 进程下使能 BFD		
4	**rip** [*process-id*] 例如：[Huawei] **rip** 100	进入 RIP 视图
5	**bfd all-interfaces enable** 例如：[Huawei-rip-100]**bfd all-interfaces enable**	在 RIP 进程下使能所有接口的 BFD 特性。当配置了全局 BFD 特性，且邻居状态为 Up 时，RIP 为该进程下所有在对应进程下的接口使用缺省的 BFD 参数值建立 BFD 会话 缺省情况下，RIP 进程的 BFD 特性未使能，可用 **undo bfd all-interfaces enable** 命令在 RIP 进程下去使能所有接口的 BFD 特性

（续表）

步骤	命令	说明
6	**bfd all-interfaces** { **min-rx-interval** *min-receive-value* | **min-tx-interval** *min-transmit-value* | **detect-multiplier** *detect-multiplier-value* } * 例如：[Huawei-rip-100] **bfd all-interfaces min-tx-interval** 500	（可选）配置 BFD 会话的参数值。命令中的参数说明如下 ● **min-rx-interval** *min-receive-value*：可多选参数，指定期望从对端接收 BFD 报文的最小接收间隔，取值范围为 10～2 000 的整数毫秒 ● **min-tx-interval** *min-transmit-value*：可多选参数，指定向对端发送 BFD 报文的最小发送间隔，取值范围为 10～2 000 的整数毫秒 ● **detect-multiplier** *detect-multiplier-value*：可多选参数，指定本地检测倍数，取值范围为 3～50 的整数 【说明】执行该命令后，所有 RIP 接口建立 BFD 会话的参数都会改变。至于以上参数的配置，请注意以下几个方面 ● 本地 BFD 报文实际发送时间间隔＝MAX｛本地配置的发送时间间隔 *transmit-value*，对端配置的接收时间间隔 *receive-value*｝ ● 本地 BFD 报文实际接收时间间隔＝MAX｛对端配置的发送时间间隔 *transmit-value*，本地配置的接收时间间隔 *receive-value*｝ ● 本地 BFD 报文实际检测时间＝本地实际接收时间间隔 × 对端配置的 BFD 检测倍数 *detect-multiplier-value* ● 对于网络可靠性要求较高的链路，可以通过配置减小 BFD 报文实际发送时间间隔；对于网络可靠性要求较低的链路，可以通过配置增大 BFD 报文实际发送时间间隔 缺省情况下，BFD 会话采用缺省参数值，即 *min-receive-value* 和 *min-transmit-value* 为 1 000 ms，*detect-multiplier-value* 为 3 倍，可用 **undo bfd all-interfaces** { **min-rx-interval** [*min-receive-value*] | **min-tx-interval** [*min-transmit-value*] | **detect-multiplier** [*detect-multiplier-value*] } *命令恢复 BFD 会话参数为缺省值
7	**quit** 例如：[Huawei-rip-100] **quit**	退出 RIP 视图，返回系统视图
8	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要阻塞创建 BFD 会话的 RIP 路由器接口，进入接口视图。**仅当有 RIP 路由器接口不需要使能 BFD 特性时配置**
9	**rip bfd block** 例如：[Huawei-GigabitEthernet1/0/0]**rip bfd block**	（可选）阻塞以上接口创建 BFD 特性 缺省情况下，不使能该阻塞功能，可用 **undo rip bfd block** 命令取消该阻塞功能
对所有不希望创建 BFD 会话的 RIP 路由器接口，均要配置步骤 8～9 来阻塞这些接口的 BFD 功能		
方式 2：在 RIP 接口下使能 BFD		
4	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet **2**/0/0	键入要使能 BFD 会话功能的 RIP 路由器接口，进入接口视图
5	**rip bfd enable** 例如：[Huawei-GigabitEthernet2/0/0]**rip bfd enable**	使能指定接口的 BFD 特性，建立缺省参数值的 BFD 会话 如果没有使能全局 BFD，接口上的 BFD 参数可以配置，但不会创建 BFD 会话，**所以必须先按本表第 2 步全局使能 BFD 会话功能** 缺省情况下，不使能 RIP 接口的 BFD 特性，可用 **undo rip bfd enable** 命令取消指定接口的 BFD 特性

（续表）

步骤	命令	说明
6	**rip bfd** { **min-rx-interval** *min-receive-value* | **min-tx-interval** *min-transmit-value* | **detect-multiplier** *detect-multiplier-value* } * 例如：[Huawei-GigabitEthernet2/0/0] **rip bfd min-tx-interval** 600 **detect-multiplier** 4	在以上接口上配置动态 BFD 会话的参数值，其中的参数说明与本表第 6 步的对应参数一致，参见即可 【说明】只有接口使能了 BFD 特性，进程中所配置的 BFD 会话参数才会生效。在接口上配置的 BFD 优先级高于在进程中配置的 BFD 优先级，如果接口配置了 BFD 参数，则按照接口上配置的 BFD 参数建立会话 缺省情况下，动态 BFD 会话参数为缺省值，即 *min-receive-value* 和 *min-transmit-value* 为 1 000 ms，*detect-multiplier-value* 为 3 倍，可用 **undo rip bfd** { **min-rx-interval** [*min-receive-value*] | **min-tx-interval** [*min-transmit-value*] | **detect-multiplier** [*detect-multiplier-value*] } *命令恢复指定接口上动态 BFD 会话参数为缺省值

2. 配置 RIP 与静态 BFD 联动

配置 RIP 与静态 BFD 联动是实现 BFD 检测功能的一种方式，可以有以下两种配置方法。

① 单臂回声 BFD：当支持 BFD 的设备与不支持 BFD 的设备对接时，可以**在单端 RIP 路由器上**通过配置静态 BFD 来实现单臂回声 BFD 检测功能。**具体参见 7.3.4 小节**。

② 普通单跳 BFD：在某些对故障响应速度要求高且两端设备都支持 BFD 的链路上，可以**在两端 RIP 路由器上**通过配置静态 BFD 来实现普通 BFD 检测功能。**具体参见 7.3.1 小节**。

RIP 与静态 BFD 联动的具体配置步骤如表 11-10 所示。

表 11-10　　配置 RIP 与静态 BFD 联动的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 全局视图
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	按照第 7 章 7.3.4 小节配置单臂回声 BFD，或者按照第 7 章 7.3.1 小节配置普通单跳 BFD	
5	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 2/0/0	键入要使能 BFD 会话功能的 RIP 路由器接口，进入接口视图
6	**rip bfd static** 例如：[Huawei-GigabitEthernet2/0/0]**rip bfd static**	在使能 RIP 的特定接口下使能静态 BFD 特性 缺省情况下，RIP 接口不使能静态 BFD 特性，可用 **undo rip bfd static** 命令在使能 RIP 的特定接口下去使能静态 BFD 特性 【说明】如果采用的是与单臂回声 BFD 的联动，则仅需要在支持 BFD 的一端 RIP 路由器接口上配置；如果采用的是与单跳 BFD 的联动，则需要在 BFD 会话的两端 RIP 路由器接口上配置

11.2.9 RIP 路由管理

配置好各项 RIP 路由功能后，可以使用以下 **display** 任意视图命令查看相关 RIP 功能配置信息，验证配置结果，也可使用以下 **reset** 用户视图命令清除相关 RIP 路由统计信息。

① **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]：查看所有或指定 RIP 进程，或者公网或指定 VPN 实例下的当前运行状态及配置信息。

② **display rip** *process-id* **route**：查看指定 RIP 进程下所有从其他设备学习到的 RIP 路由。

③ **display default-parameter rip**：查看 RIP 的缺省配置信息。

④ **display rip** *process-id* **statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ip-address*] }：查看指定 RIP 进程下指定或所有 RIP 路由器接口的统计信息。

⑤ **display rip** *process-id* **database** [**verbose**]：查看指定 RIP 进程下 RIP 数据库中的所有激活路由。

⑥ **display rip** *process-id* **interface** [*interface-type interface-number*] [**verbose**]：查看所有或者指定 RIP 进程下的接口信息。

⑦ **display rip** *process-id* **neighbor** [**verbose**]：查看指定 RIP 进程下的邻居信息。

⑧ **reset rip** *process-id* **configuration**：复位指定 RIP 进程的系统配置参数，这样当 RIP 进程启动时，所有配置参数将采用缺省值。

⑨ **reset rip** *process-id* **statistics interface** { **all** | *interface-type interface-number* [**neighbor** *neighbor-ip-address*] }：清除所有或者指定 RIP 进程维护的计数器的统计数据。

11.2.10 RIP 基本功能配置示例

本示例的基本拓扑结构如图 11-18 所示，在网络中有 4 台路由器，要求在 RouterA、RouterB、RouterC 和 RouterD 上通过 RIP 协议实现网络互联。

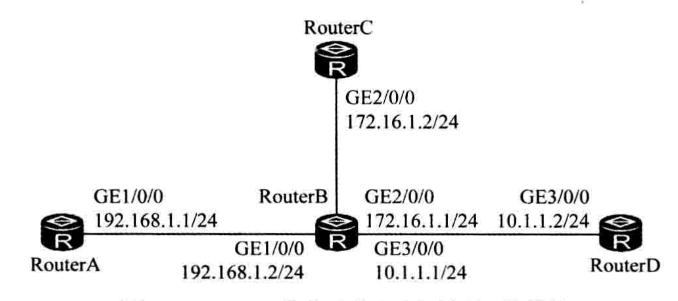


图 11-18 RIP 基本功能配置示例拓扑结构

1. 基本配置思路分析

这是一个很简单的 RIP 路由配置示例，仅需通过 RIP 路由的基本功能就可以实现这 4 台路由器的互通。其基本的配置思路如下。

① 配置各路由器接口 IP 地址，使网络可达。

② 在各路由器上创建 RIP 进程（**各路由器的 RIP 进程号可以不一样，因为路由进程号仅在本地有意义**，本书后面介绍的其他路由协议的进程号也一样），并宣告要使能 RIP 的接口所对应的自然网段。

③ 在各路由器上配置 RIP 版本（建议为 RIPv2 版本），以提升 RIP 路由扩展性能。

2. 具体配置步骤

① 按照图中标注配置各路由器接口的 IP 地址。仅以 RouterA 上的接口 IP 地址为例进行介绍，RouterB、RouterC 和 RouterD 的接口 IP 地址配置方法与 RouterA 的一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
```

② 配置 RIP 基本功能，创建 RIP 进程号，宣告各 RIP 路由器接口对应的自然网段。

RouterA 上的配置如下。

```
[RouterA] rip
[RouterA-rip-1] network 192.168.1.0
[RouterA-rip-1] quit
```

RouterB 上的配置如下。

```
[RouterB] rip
[RouterB-rip-1] network 192.168.1.0
[RouterB-rip-1] network 172.16.0.0
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] quit
```

RouterC 上的配置如下。

```
[RouterC] rip
[RouterC-rip-1] network 172.16.0.0
[RouterC-rip-1] quit
```

RouterD 上的配置如下。

```
[RouterD] rip
[RouterD-rip-1] network 10.0.0.0
[RouterD-rip-1] quit
```

配置好后，可以通过 **display rip route** 命令查看各路由器的 RIP 路由表。下面是 RouterA 的 RIP 路由表。从路由表中可以看出，因为目前还没有配置 RIPv2 版本，所以可见 RIPv1 发布的路由信息使用的是自然掩码。

```
[RouterA] display rip 1 route
 Route Flags: R - RIP
              A - Aging, S - Suppressed, G - Garbage-collect
-------------------------------------------------------------------------
 Peer 192.168.1.2    on GigabitEthernet1/0/0
      Destination/Mask        Nexthop       Cost   Tag    Flags   Sec
        10.0.0.0/8            192.168.1.2     1     0      RA      14
        172.16.0.0/16         192.168.1.2     1     0      RA      14
```

③ 在各 RIP 路由器上 RIPv2 版本，因为各路由器上的配置完全一样，故仅以 RouterA 上的 RIPv2 版本配置为例进行介绍，RouterB、RouterC 和 RouterD 的配置，略。

```
[RouterA] rip
[RouterA-rip-1] version 2
[RouterA-rip-1] quit
```

现使用 **display rip 1 route** 命令查看 RouterA 的 RIP 路由表。此时，从路由表中可以看出，RIPv2 发布的路由中带有更为精确的子网掩码信息。

```
[RouterA] display rip 1 route
  Route Flags: R - RIP
               A - Aging, S - Suppressed, G - Garbage-collect
-------------------------------------------------------------------------
 Peer 192.168.1.2   on GigabitEthernet1/0/0
      Destination/Mask        Nexthop       Cost   Tag     Flags    Sec
         10.1.1.0/24         192.168.1.2      1     0        RA      32
         172.16.1.0/24       192.168.1.2      1     0        RA      32
```

11.2.11 RIP 引入外部路由配置示例

本示例的基本拓扑结构如图 11-19 所示，RouterB 上运行两个 RIP 进程：RIP100 和 RIP200。要求通过两个 RIP 进程的路由相互引入实现 RouterA 与 192.168.3.0/24 网段互通，但不要与 192.168.4.0/24 网段互通。

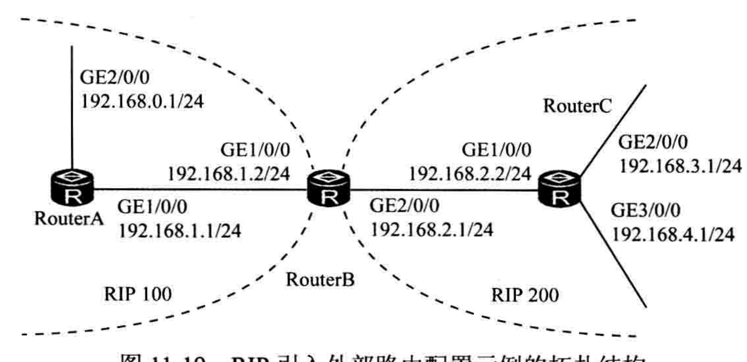


图 11-19 RIP 引入外部路由配置示例的拓扑结构

1. 基本配置思路分析

本示例采用两个不同进程的 RIP 路由相互引入来实现不同进程中的网络互通。要特别注意的是，外部路由的引入仅需在同时属于内、外部网络的路由器上进行配置，其基本配置思路如下。

① 在各路由器上使能 RIP，实现各进程内的网络互联。

② 在 RouterB 上配置 RIP100 和 RIP200 之间的路由相互引入，将引入的 RIP200 路由的缺省权值设为 3，实现两进程路由互通。

③ 在 RouterB 上配置 ACL，对引入的 RIP200 的 192.168.4.0/24 网络路由进行过滤，使 RouterA 仅与网段 192.168.3.0/24 互通。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址，此处仅以 RouterA 的配置为例，RouterB 和 RouterC 的配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
```

② 在 RouterA、RouterB、RouterC 上分别配置 RIP 基本功能。要在 RouterA 上启动 RIP 进程 100，在 RouterC 上启动 RIP 进程 200，而在 RouterB 上要同时启动这两个 RIP 进程，然后分别宣告这些 RIP 接口直连网段对应的自然网段。

```
[RouterA] rip 100
[RouterA-rip-100] network 192.168.0.0
[RouterA-rip-100] network 192.168.1.0
```

```
[RouterA-rip-100] quit
[RouterB] rip 100
[RouterB-rip-100] network 192.168.1.0
[RouterB-rip-100] quit
[RouterB] rip 200
[RouterB-rip-200] network 192.168.2.0
[RouterB-rip-200] quit
[RouterC] rip 200
[RouterC-rip-200] network 192.168.2.0
[RouterC-rip-200] network 192.168.3.0
[RouterC-rip-200] network 192.168.4.0
[RouterC-rip-200] quit
```

此时在 RouterA 上可通过命令查看 IP 路由表信息，发现并没有 RIP 200 进程下的路由。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct  0    0           D   192.168.0.1     GigabitEthernet2/0/0
    192.168.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
```

③ 在 RouterB 上设置缺省路由值为 3（以便从 RIP 进程 200 中引入的路由优先于其他协议的路由在 RIP 进程 100 中进行发布），并将两个不同 RIP 进程的路由相互引入到对方的路由表中。

```
[RouterB] rip 100
[RouterB-rip-100] default-cost 3
[RouterB-rip-100] import-route rip 200
[RouterB-rip-100] quit
[RouterB] rip 200
[RouterB-rip-200] import-route rip 100
[RouterB-rip-200] quit
```

此时再来查看 RouterA 的 IP 路由表信息，发现 RIP 进程 200 中的路由已在 RouterA 的 IP 路由表中了。它们的开销值要在配置的缺省值 3 的基础上再加 1，最终等于 4（**参见输出信息中的粗体字部分**）。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct  0    0           D   192.168.0.1     GigabitEthernet2/0/0
    192.168.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
```

```
192.168.2.0/24  RIP    100  4        D   192.168.1.2     GigabitEthernet1/0/0
192.168.3.0/24  RIP    100  4        D   192.168.1.2     GigabitEthernet1/0/0
192.168.4.0/24  RIP    100  4        D   192.168.1.2     GigabitEthernet1/0/0
```

④ 在 RouterB 上配置 ACL，并增加一条规则：拒绝源地址为 192.168.4.0/24 的报文。

```
[RouterB] acl 2000
[RouterB-acl-basic-2000] rule deny source 192.168.4.0 0.0.0.255
[RouterB-acl-basic-2000] rule permit
[RouterB-acl-basic-2000] quit
```

然后在 RouterB 上应用前面配置的 ACL 2000，以控制在向 RouterA 发布路由更新时，过滤引入的 RIP 进程 200 的路由 192.168.4.0/24。

```
[RouterB] rip 100
[RouterB-rip-100] filter-policy 2000 export
[RouterB-rip-100] quit
```

最后再检查过滤后的 RouterA 上的 IP 路由表，发现已没有原来的 192.168.4.0/24 网段路由了（**如粗体字部分显示**），表示过滤成功。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9          Routes : 9
Destination/Mask    Proto   Pre  Cost       Flags NextHop         Interface
      127.0.0.0/8   Direct  0    0            D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0            D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct  0    0            D   192.168.0.1     GigabitEthernet2/0/0
    192.168.0.1/32  Direct  0    0            D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0            D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.1/32  Direct  0    0            D   127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct  0    0            D   192.168.1.2     GigabitEthernet1/0/0
    192.168.2.0/24  RIP     100  4            D   192.168.1.2     GigabitEthernet1/0/0
    192.168.3.0/24  RIP     100  4            D   192.168.1.2     GigabitEthernet1/0/0
```

11.2.12 RIP 与单臂回声静态 BFD 联动特性的配置示例

本示例的基本拓扑结构如图 11-20 所示，在小型网络中有 4 台路由器通过 RIP 实现网络互通。其中业务流量经过主链路 RouterA→RouterB→RouterD 进行传输。现为了提高从 RouterA 到 RouterB 数据转发的可靠性，要求当主链路发生故障时，业务流量会快速切换到经由 RouterC 的另一条路径进行传输。现假设 RouterB 不支持 BFD。

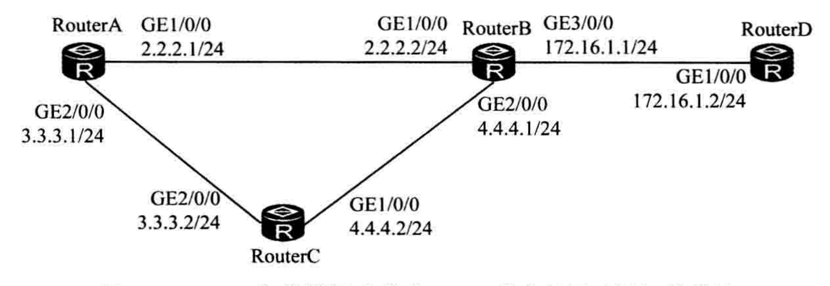


图 11-20 RIP 与单臂回声静态 BFD 联动配置示例拓扑结构

1. 基本配置思路分析

因为 RouterB 不支持 BFD，所以只能采用与单臂回声静态 BFD 联动的方式。其基

本的配置思路如下。

① 在各接口上配置 IP 地址，使网络可达。

② 在各路由器上使能 RIP，基本实现网络互联。

③ 在 RouterA 上配置 RIP 与单臂回声静态 BFD 联动，通过 BFD 快速检测 RouterA 到 RouterB 之间的主链路状态，从而提高 RIP 的收敛速度，实现链路的快速切换。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。仅以 RouterA 进行介绍，RouterB、RouterC 和 RouterD 的配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 2.2.2.1 24
```

② 配置 RouterA、RouterB、RouterC 和 RouterD 的 RIP 基本功能，宣告它们各自直连网段所对应的自然网段，然后把它们的 RIP 版本号配置为 2，以提高它们的可扩展性。

```
<RouterA> system-view
[RouterA] rip 1
[RouterA-rip-1] version 2
[RouterA-rip-1] network 2.0.0.0
[RouterA-rip-1] network 3.0.0.0
[RouterA-rip-1] quit

<RouterB> system-view
[RouterB] rip 1
[RouterB-rip-1] version 2
[RouterB-rip-1] network 2.0.0.0
[RouterB-rip-1] network 4.0.0.0
[RouterB-rip-1] network 172.16.0.0
[RouterB-rip-1] quit

<RouterC> system-view
[RouterC] rip 1
[RouterC-rip-1] version 2
[RouterC-rip-1] network 3.0.0.0
[RouterC-rip-1] network 4.0.0.0
[RouterC-rip-1] quit

<RouterD> system-view
[RouterD] rip 1
[RouterD-rip-1] version 2
[RouterD-rip-1] network 172.16.0.0
[RouterD-rip-1] quit
```

此时可通过 **display rip neighbor** 命令查看 RouterA、RouterB 以及 RouterC 之间已经建立的邻居关系。下面是 RouterA 上的输出示例。

```
[RouterA] display rip 1 neighbor
---------------------------------------------------------------------

  IP Address       Interface              Type   Last-Heard-Time
---------------------------------------------------------------------
  2.2.2.2          GigabitEthernet1/0/0    RIP    0:0:1
  Number of RIP routes   : 1
  3.3.3.2          GigabitEthernet2/0/0    RIP    0:0:2
  Number of RIP routes   : 2
```

可通过 **display ip routing-table** 命令查看各 RIP 路由器的 IP 路由表信息。下面是 RouterA 上的输出示例。从中可以看出，去往 172.16.0.0/16 网段的下一跳 IP 地址是 RouterB 的 GE1/0/0 接口中的 IP 地址 2.2.2.2，出接口是 RouterA 的 GE1/0/0。即流量在主链路 RouterA→RouterB 上进行传输，因为这条路由的开销（1）比起经由 RouterC 再到达 RouterB 的路由开销（2）要小。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8          Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        2.2.2.0/24  Direct  0    0           D   2.2.2.1         GigabitEthernet1/0/0
        2.2.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
        3.3.3.0/24  Direct  0    0           D   3.3.3.1         GigabitEthernet2/0/0
        3.3.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
        4.0.0.0/8   RIP     100  1           D   2.2.2.2         GigabitEthernet1/0/0
                    RIP     100  1           D   3.3.3.2         GigabitEthernet2/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.0.0/16   RIP     100  1           D   2.2.2.2         GigabitEthernet1/0/0
```

③ 在 RouterA 上配置以 RouterB 的 GE1/0/0 接口为对端的单臂回声静态 BFD 会话。要求同时绑定对端 IP 地址和本地出接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd 1 bind peer-ip 2.2.2.2 interface gigabitethernet 1/0/0 one-arm-echo
[RouterA-session-1] discriminator local 1
[RouterA-session-1] min-echo-rx-interval 200
[RouterA-session-1] commit
[RouterA-session-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] rip bfd static   !—使能本地 GigabitEthernet1/0/0 接口的静态 BFD 功能
[RouterA-GigabitEthernet1/0/0] quit
```

完成上述配置之后，在 RouterA 上执行 **display bfd session all** 命令，可以看到静态 BFD 会话已经建立。

```
[RouterA] display bfd session all
--------------------------------------------------------------------------------
Local  Remote  PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
1      -       2.2.2.2         Up        S_IP_IF     GigabitEthernet1/0/0
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

在 RouterB 的接口 GigabitEthernet1/0/0 上执行 **shutdown** 命令，模拟主链路故障。然后通过 **display bfd session all** 命令查看 RouterA 的 BFD 会话信息，可以看到 RouterA 及 RouterB 之间已不存在 BFD 会话信息了。

如果通过 **display ip routing-table** 命令查看 RouterA 的 IP 路由表，就会发现，在主链路发生故障后备份链路 RouterA→RouterC→RouterB 被启用，去往 172.16.0.0/16 网段的路由下一跳 IP 地址是 RouterC 的 GE2/0/0 接口 IP 地址 3.3.3.2，出接口为 RouterA 的

GE2/0/0 接口（**参见输出信息中的粗体字部分**），表明切换成功。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6          Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      3.3.3.0/24    Direct  0    0           D   3.3.3.1         GigabitEthernet2/0/0
      3.3.3.1/32    Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
      4.0.0.0/8     RIP     100  1           D   3.3.3.2         GigabitEthernet2/0/0
    127.0.0.0/8     Direct  0    0           D   127.0.0.1       InLoopBack0
    127.0.0.1/32    Direct  0    0           D   127.0.0.1       InLoopBack0
   172.16.0.0/16    RIP     100  2           D   3.3.3.2         GigabitEthernet2/0/0
```

11.2.13 RIP 与动态 BFD 联动特性的配置示例

本示例的基本拓扑结构参见图 11-20，其中业务流量经过主链路 RouterA→RouterB→RouterD 进行传输，备份链路为 RouterA→RouterC→RouterB→RouterD。与上一示例唯一的区别在于现在 RouterB 已支持 BFD，且要求采用 RIP 与动态 BFD 联动以实现主备链路切换。

本示例采用的是 RIP 与动态 BFD 联动的方式，要求分别在 RouterA 和 RouterB 上配置 RIP 与动态 BFD 联动，其他的各路由器接口 IP 地址和 RIP 基本功能配置与上一示例完全一样，参见即可。故在此仅介绍在 RouterA 和 RouterB 上配置动态 BFD 会话以及 RIP 与动态 BFD 联动的部分。

配置 RouterA 上所有接口的 BFD 特性，RouterB 的配置与此相同，略。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] rip 1
[RouterA-rip-1] bfd all-interfaces enable
[RouterA-rip-1] bfd all-interfaces min-rx-interval 100 min-tx-interval 100 detect-multiplier 10
[RouterA-rip-1] quit
```

完成配置之后，在路由器上执行 **display rip bfd session** 命令，可以看到 RouterA 与 RouterB 之间已经建立起 BFD 会话。下面是 RouterA 上的输出示例，从中可以看出 BFDState 字段显示为 Up（**参见输出信息中的粗体字部分**）。

```
[RouterA] display rip 1 bfd session all
 LocalIp        :2.2.2.1        RemoteIp   :2.2.2.2        BFDState :Up
 TX             :100            RX         :100            Multiplier:10
 BFD Local Dis:8192             Interface  :GigabitEthernet1/0/0
 DiagnosticInfo: No diagnostic information
 LocalIp        :3.3.3.1        RemoteIp   :3.3.3.2        BFDState :Down
 TX             :0              RX         :0              Multiplier:0
 BFD Local Dis :8200            Interface :GigabitEthernet2/0/0
 Diagnostic Info:No diagnostic information
```

在 RouterB 的接口 GigabitEthernet1/0/0 上执行 **shutdown** 命令，模拟主链路故障。然后通过执行 **display rip bfd session** 命令查看 RouterA 的 BFD 会话信息，可以看到 RouterA 及 RouterB 之间不存在 BFD 会话信息。

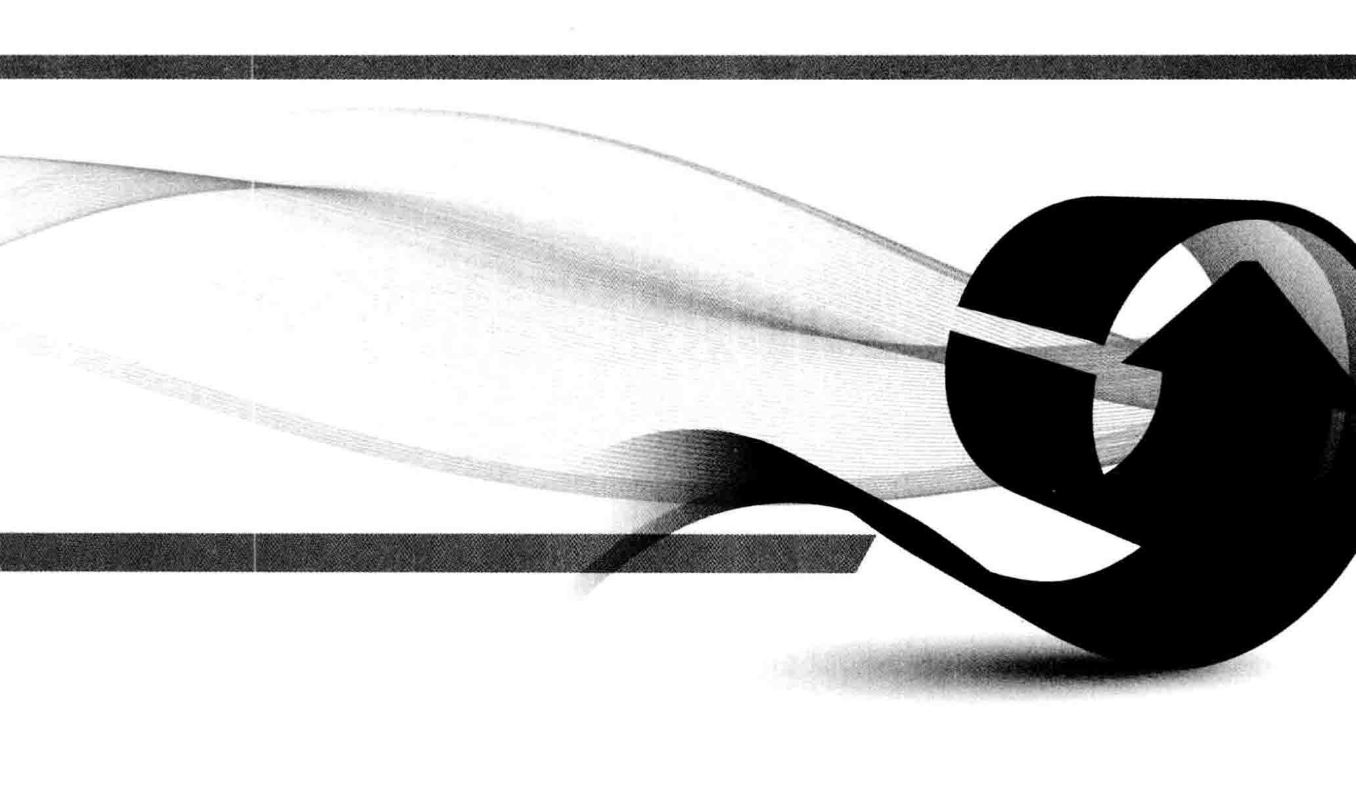
```
[RouterA] display rip 1 bfd session all
 LocalIp        :3.3.3.1          RemoteIp  :3.3.3.2          BFDState  :Down
 TX             :0                RX        :0                Multiplier:0
 BFD Local Dis :8200              Interface :GigabitEthernet2/0/0
 Diagnostic Info:No diagnostic information
```

如果通过 **display ip routing-table** 命令查看 RouterA 的 IP 路由表，就会发现，当主链路发生故障后备份链路 RouterA→RouterC→RouterB 被启用，去往 172.16.0.0/16 网段的路由下一跳 IP 地址是 RouterC 的 GE2/0/0 接口 IP 地址 3.3.3.2，出接口为 RouterA 的 GE2/0/0 接口（**参见输出信息中的粗体字部分**），表明切换成功。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6          Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       3.3.3.0/24   Direct  0    0           D   3.3.3.1         GigabitEthernet2/0/0
       3.3.3.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
       4.0.0.0/8    RIP     100  1           D   3.3.3.2         GigabitEthernet2/0/0
     127.0.0.0/8    Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.0.0/16   RIP     100  2           D   3.3.3.2         GigabitEthernet2/0/0
```



第12章
OSPF路由配置与管理

12.1 OSPF基础

12.2 OSPF报头及各种报文格式

12.3 OSPF工作原理

12.4 配置OSPF基本功能

12.5 配置OSPF邻居或邻接的会话参数

12.6 配置OSPF在不同网络类型中的属性

12.7 配置OSPF的Stub/Totally Stub/NSSA/Totally NSSA区域

12.8 配置OSPF安全功能

12.9 调整OSPF的路由选择

12.10 控制OSPF路由信息的发布和接收

12.11 调整OSPF网络收敛性能

12.12 配置OSPF与BFD联动



OSPF（开放式最短路径优先）是一个基于链路状态进行路由计算的动态路由协议，主要用于大中型网络。目前，华为AR G3系列路由器主要支持OSPFv2和OSPFv3两种版本，OSPFv2仅支持IPv4，而OSPFv3同时支持IPv4和IPv6。**本书仅介绍基于IPv4网络的OSPFv2版本。**

相对上一章介绍的RIP动态路由协议来说，OSPF路由的配置更为复杂，功能也更为强大。其显著特点就是不仅可以在一台路由器上运行多种OSPF路由进程，还可把一个AS（自治系统）划分成多个不同的Area（区域），然后基于路由器的位置和功能划分多种不同的OSPF路由器类型和OSPF路由类型，同时支持不同类型网络的连接。但OSPF仍与RIP一样，是一种IGP（内部网关协议）类型动态路由协议，所以OSPF路由也只用于一个AS内部。总体来说，OSPF是通过LSA（链路状态通告）报文进行路由信息交互，通过5种报文（Hello、DBD、LSR、LSU、LSAck）进行邻居和邻接关系的建立以及同一区域内部各路由器间的LSDB（链路状态数据库）信息的同步，最终形成统一的区域内拓扑数据库。

本章将比较全面地介绍OSPFv2的基础知识、工作原理以及各主要功能特性（如OSPF基本功能、OSPF网络类型、OSPF区域类型、OSPF安全验证、OSFP路由信息发布和接收过滤、OSPF的路由选择、OSPF路由聚合、OSPF外部路由引入、OSPF LSA发布过滤、OSPF与BFD的联动等）的配置思路和步骤，同时给出大量的具体配置示例，以巩固对各功能配置方法的学习。

12.1 OSPF 基础

OSPF（Open Shortest Path First，开放式最短路径优先）协议是 IETF 组织开发的一个基于链路状态的 AS 内部的 IGP（内部网关协议），广泛应用在接入网和城域网中。

在 OSPF 出现前，网络上广泛使用 RIP 作为内部网关协议。但由于 RIP 是基于距离矢量算法的路由协议，存在着收敛慢、路由环路、可扩展性差等问题，所以最终逐渐被可全面解决 RIP 的这些问题的 OSPF 所取代。目前，针对 IPv4 协议使用的是 OSPFv2（RFC2328）版本；针对 IPv6 协议使用 OSPFv3（RFC2740）版本。如无特殊说明，本章中所指的 OSPF 均为 OSPFv2 版本。

12.1.1 OSPF 的几个重要概念

要认识 OSPF，首先就要了解 OSPF 的几个非常重要的基本概念：自治系统（AS）、区域（Area）、路由器类型和路由类型。首先要说明的是，一台运行 OSPF 协议路由器中的每个 OSPF 进程必须指定一个用于标识本地路由器的 Router ID（路由器 ID）。Router ID 是一个 32 比特无符号整数。**在一个 AS 中每个路由器 ID 必须唯一，但同一路由器的不同进程中的路由器 ID 可以相同。**

1. AS

AS（自治系统）也就是通常所讲的"路由域"（Routing Domain），是由运行同一种路由协议并且被同一组织机构管理的一组路由器组成。**同一个 AS 中的所有路由器必须运行相同的路由协议，且必须彼此相互连接（中间不能被其他协议路由域所间断），分配相同的 AS 号**。不仅 OSPF 可以配置 AS，IS-IS、BGP 等动态路由协议也可以配置 AS，都可以形成特定的路由域。

在 OSPF 网络中，只有在同一 AS 中的路由器才会相互交换链路状态信息；在同一个 AS 中，所有的 OSPF 路由器都维护一个相同 AS 结构描述（就是 AS 中各区域间的连接关系）的数据库。该数据库中存放的是路由域中相应链路的状态信息，然后 OSPF 通过这个数据库计算出其 OSPF 路由表。我们所进行的 OSPF 路由配置都是针对同一个 AS 内部的路由器之间进行配置的，不涉及不同 AS 之间的路由器间的路由。本书后面将要介绍担当不同 AS 间路由的 BGP 协议的任务。

2. Area

Area（区域）是 OSPF 的一个非常重要的特征，就是在一个 AS 内部划分的多个不同位置，或者不同角色的一组路由器单元，**每个 OSPF 路由器只能在所属区域内部学习到完整的链路状态信息**。在大中型网络中，路由器设备可能非常多，如果不进行区域划分的话，则整个网络中的所有设备都要彼此学习路由信息，最终所生成的路由信息数据库就可能非常庞大，这样既大大消耗了路由器的有限存储空间，也不利于进行高效路由选择。当然，区域的划分也不是随意进行的，是要根据这些路由器在网络中承担的作用和位置来划分的，具体将在下节介绍。

图 12-1 所示为 Area 与 AS 之间的关系示意图，即一个 AS 中可以包括多个区域，不同的协议路由域使用不同的 AS。**但只有 OSPF 和 IS-IS 协议路由域中的 AS 可以划分多**

个区域。不同路由域（也即不同 AS）中的路由需要经过本书后面第 14 章中介绍的 BGP 协议进行连接。

区域是从逻辑上将网络中的不同路由设备划分为不同的组，每个组用区域号（Area ID）来标识。但要注意的是，OSPF 的区域的边界是设备接口，而不是链路。即一个网段（链路）只能整个属于同一个区域，**即路由器间直接相连的链路两端接口必须属于同一个区域**，如图 12-2 所示。划分了区域后，可以在区域边界路由器上进行路由聚合，不同区域之间仅向外通告其聚合路由，这样就可以大大减少通告到其他区域的 LSA（链路状态通告）数量。另外，还可以最小化由于网络拓扑变化带来的影响。

说明　与 OSPF 同为链路状态协议的 IS-IS 在区域边界方面就与 OSPF 完全相反，IS-IS 区域的边界恰好是链路，而不是设备接口，即两台路由器相连的链路两端接口是分属于不同区域的，有关 IS-IS 路由将在本书下一章具体介绍。

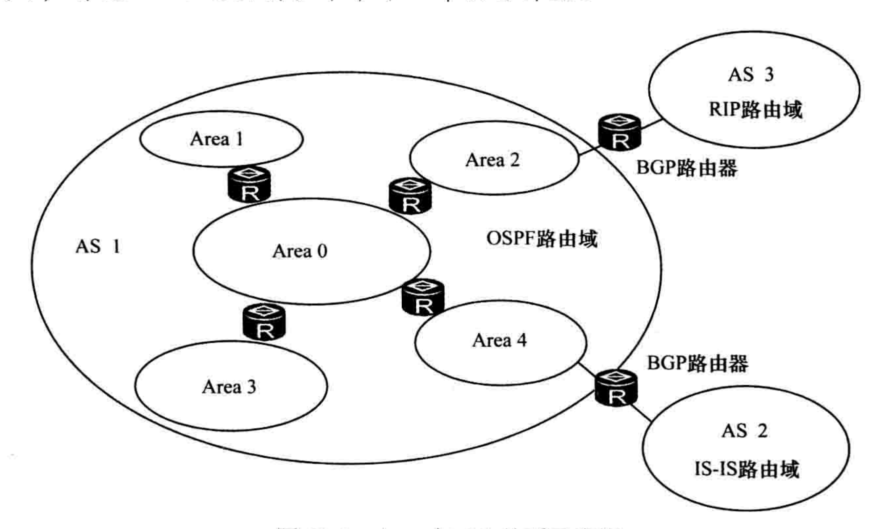


图 12-1　Area 与 AS 关系示意图

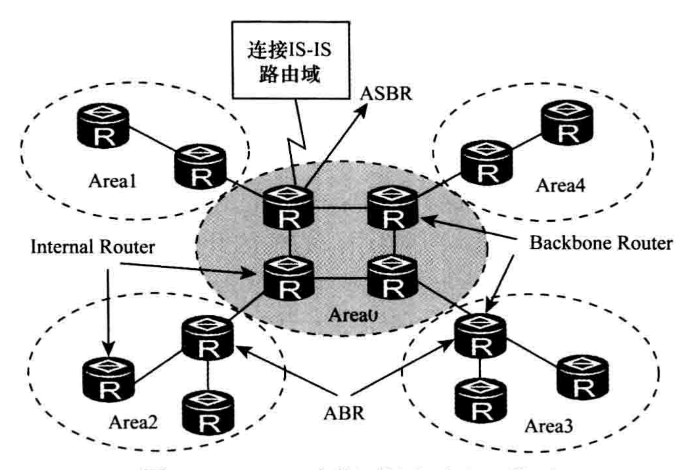


图 12-2　OSPF 中的区域和路由器类型

在 OSPF 中，除了可以划分多个普通区域外，还可以配置多种特殊区域类型，如骨

干区域（固定为 Area0）、Stub（末梢）区域、Totally Stub（完全末梢）区域、NSSA（非纯末梢）区域和 Totally NSSA（完全非纯末梢）区域，具体将在本章后面详细介绍。

3. 路由器类型

由于 OSPF 把一个 AS 划分成了多个区域，这就使得 OSPF 网络中不同路由器的角色可能会有所不同。根据路由器在 AS 中的不同位置，可以分为以下 4 类（参见图 12-2）。

① 区域内路由器（Internal Routers，IR）：该类设备的**所有接口都在同一个 OSPF 区域内**。

② 区域边界路由器（Area Border Routers，ABR）：该类设备接口**可以分别属不同区域，但其中一个接口必须连接骨干区域**。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接（也就是“虚连接”）。

③ 骨干路由器（Backbone Routers，BR）：该类设备**至少有一个接口属于骨干区域。所有的 ABR 和位于骨干区域的内部设备都是骨干路由器**。

④ 自治系统边界路由器（AS Boundary Routers，ASBR）：与其他 AS 中的设备交换路由信息的设备称为 ASBR。**虽然 ASBR 通常是位于 AS 的边界，但也可以是区域内设备，也可以同时是 ABR**。只要一台 OSPF 设备引入了外部路由（包括直连路由、静态路由、RIP、IS-IS 路由、BGP 路由，或者其他 OSPF 进程路由等）的信息，它就成为 ASBR。

4. 路由类型

划分区域的目的就是想减少 LSA 的数量，减少路由器上依据 LSA 形成的路由数量，这就自然会想到对在区域内部，或者区域之间，甚至从其他 AS 外入的路由进行分类。在 OSPF 中，把路由分成以下 4 类。

① 区域内（Intra Area）路由：**仅用于区域内 IR 路由器之间的路由**，用于 IR 设备间的互联，不向区域外通告。

② 区域间（Inter Area）路由：**仅用于区域间 ABR 之间的路由**，用于骨干区域与其他区域相互通告路由信息。

③ 第一类外部（Type1 External）路由：这是经由 ASBR 引入的外部路由，且通常是 IGP 类型（如直连路由、静态路由、RIP、IS-IS 路由或者其他 OSPF 进程路由）的外部路由，它们的开销值计算方法与 OSPF 的开销值计算方法具有可比性，可信度较高。**到第一类外部路由的开销=本设备到相应的 ASBR 的开销+ASBR 到该路由目的地址的开销**。

④ 第二类外部（Type2 External）路由：这也是经由 ASBR 引入的外部路由，且通常是 EGP 类型（如 BGP 路由）的外部路由，它们的开销值计算方法与 OSPF 的开销值计算方法不具有可比性，可信度较低。OSPF 协议认为，从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销，所以 OSPF 计算第二类外部路由的开销时只考虑 ASBR 到自治系统之外的开销，即**到第二类外部路由的开销=ASBR 到该路由目的地址的开销**。

说明 以上第一类外部路由和第二类外部路由不是由系统自动判定的，而是由管理员依据上述两种路由的特性手动设置的，缺省为第二类外部路由。

12.1.2　OSPF 网络的设计考虑

如前所述，OSPF 比 RIP 复杂许多，主要表现在 OSPF 可以支持更大规模的网络（有更多的路由器）；另外，OSPF 还可以把网络中的路由器划分成不同的区域、不同的路由器角色，结构更复杂。这就决定了，在配置 OSPF 路由之前必须先设计好相关的 OSPF 网络，然后才能进行各方面的 OSPF 路由配置工作，而不是像 RIP 路由那样基本上不需要设计，可直接在需要启用 RIP 路由进程的路由器上进行相关的 RIP 路由配置任务。

1. OSPF 网络的设计规划

对于一个可适用于大型广域网络的复杂动态路由协议，在配置之前必须作好整个 OSPF 网络的规划工作，具体如下。

（1）确定需运行 OSPF 协议的路由器

在设计 OSPF 网络时，首先要确定的是哪些路由器的接口要启用 OSPF 路由进程。这个相对来说比较好确定，因为通常来说，在一个自治系统内部各路由器上需运行相同的动态路由协议，所以绝大多数情况下是自治系统内部的各个路由器上都要运行 OSPF 协议。

（2）合理地划分 OSPF 区域

随着网络规模日益扩大，当一个大型网络中的路由器都运行 OSPF 协议时，LSDB（链路状态数据库）会占用大量的存储空间，并使得运行 SPF（Shortest Path First，最短路径优先）算法的复杂度增加，导致 CPU 负担加重。同时，在网络规模增大之后，拓扑结构发生变化的概率也增大，网络会经常处于“振荡”之中，造成网络中会有大量的 OSPF 协议报文在传递，降低了网络的带宽利用率。更为严重的是，每一次变化都会导致网络中所有的路由器重新进行路由计算。OSPF 协议通过将一个自治系统划分成不同的区域来解决上述问题。按一般经验，在一个区域内路由器的数量最好不要超过 50 台，且当网络中的路由器的台数少于 20 台的时候，也可以只划分一个区域，即骨干区域。

另外，根据 OSPF 协议规定，所有的其他区域均必须与骨干区域连接，所以在规划区域时候应该合理地选择骨干区域的位置。通常是将骨干区域置于网络的中央，这样可以使更多的其他区域与骨干区域直接连接。当然，如果实在有不能直接与骨干区域连接的区域，则需要使用虚连接来解决。同时，由于骨干区域中的路由器要负责整个 OSPF 网络各个区域的路由信息传输，负荷比较大，所以骨干区域中的路由器应该选择性能好，处理能力强的高端路由器来承担。

（3）注意 ABR 和 ASBR 的性能要求

在 OSPF 网络中的每个 ABR 都要负责所连接的两个或多个区域间的路由信息传输工作，需要保存每个连接区域的 LSDB，而 ASBR 更是要负责两个或多个自治系统间的路由信息传输，需要保存每个连接自治系统的 LSDB，负担都非常重，所以 ABR 通常也要由性能比较高的路由器来承担。ASBR 的性能要求更高。同时因为一个 ABR 可以连接多个区域，为了不使 ABR 的负担太重，通常建议在一台 ABR 上一般最多连接 3 个区域，即一个骨干区域和两个普通区域。ASBR 类似，一个 ASBR 不要连接太多的自治系统。

2. OSPF 区域划分原则

OSPF 网络不同区域的划分不是随意的，一般可以遵循以下几个方面的原则。

（1）按照地理区域或者行政管理单位来划分

因为 OSPF 网络主要应用于广域网系统，所以它一般是跨市、跨省，甚至遍布全国、全球的。面对这样一个大的 OSPF 网络，最简单的区域划分原则就是根据各路由器所在的地理区域（区域单位可以是市、省，甚至国家，或者其他区域形式），或者以行政管理单位来划分。

（2）按照网络中的路由器性能来划分

一个 OSPF 网络中的设备往往不是同一个档次，一般也可以按照交换机那样分为接入层、汇聚层和核心层这三个大的层次，它们对应的路由器性能相应地被分为低，中，高三个档次。在 OSPF 网络区域划分中通常是将一台高端路由器下面连接的多个中段或者低端路由器划分在一个区域，这样划分的好处是可以合理地选择 ABR（区域分界路由器）。

（3）按照 IP 网段来划分

在实际的 OSPF 网络中，整个网络的 IP 地址被划分成不同的子网，这时我们就可以根据不同的网段来划分 OSPF 区域。比如我们可以连接位于同一自然网段网络之下的各个子网（如 172.16.0.0/18）。这样划分的好处是便于在 ABR 上配置路由汇聚，减少网络中路由信息的数量。

（4）区域中路由器数的考虑

通常情况下认为，在 OSPF 的一个区域中最好不要超过 50 台路由器。但现在的路由器 CPU 处理速度，内存容量都在日益增强，有测试表明，200 台路由器一个区域都可以非常快速地收敛。

12.1.3 OSPF LSA 类型

OSPF 是一种典型的链路状态路由协议，缺省情况下，采用 OSPF 的每个路由器通过向邻居路由器发送 LSA（Link State Advertisement，链路状态通告）来实现彼此交换并保存整个网络的链路状态信息，从而掌握全网的拓扑结构，**并独立计算路由**。划分区域后，OSPF 路由器收集其所在网络区域上各路由器的链路状态信息，并生成链路状态数据库（LSDB），也称为拓扑数据库，因为它代表了对应区域中的网络拓扑结构。然后 OSPF 路由器根据自己的 LSDB 利用 SPF（Shortest Path First，最短路径优先）路由算法独立地计算出到达任意目的地的路由。也就是说 LSA 是 OSPF 计算路由的依据，在相当程度上就代表了 OSPF 路由。

因为在 OSPF 网络中对各 OSPF 路由器根据其用途进行了分类，所以不同类型的 OSPF 路由器所发送的 LSA 的用途和可以通告的范围各不相同。OSPF 将 LSA 分为以下几类。

（1）Type1 LSA：路由器 LSA（Router LSA）

每个 OSPF 路由器都会产生路由器 LSA，描述了对应设备物理接口所连接的链路或接口，并且指明了各链路的状态、开销等参数。

（2）Type2 LSA：网络 LSA（Network LSA）

网络 LSA 由 DR（指定路由器）或者 BDR（备份指定路由器）产生，描述了 DR 和 BDR 所在网段的链路状态，也仅在所属的区域内传播。**因为 DR 和 BDR 仅在广播类型**

网络中存在，所以网络 LSA 也仅在广播类型网络中存在。有关广播类型网络将在本章后面具体介绍。

（3）Type3 LSA：网络聚合 LSA（Network summary LSA）

网络汇总 LSA 由 ABR 产生，描述所连接的某个区域内某个网段的聚合路由（包括缺省路由），**并通告非 Totally Stub 或 NSSA 区域（包括源网段所在区域，**到达其他区域必须经过骨干区域转发该 LSA），这样区域通信在到达区域边界 ABR 后都是采用聚合路由进行的，可大大减少区域内部路由器的路由表项数量。

（4）Type4 LSA：ASBR 聚合 LSA（ASBR summary LSA）

ASBR 聚合 LSA 也由 ABR 产生，描述从该 ABR 到达 OSPF 路由域中各个 ASBR 的路由，通告给整个路由域。**但仅可向普通区域中泛洪，**不能进入 Stub 区域、Totally Stub 区域、NSSA 区域和 Totally NSSA 区域。有关 Stub 区域、Totally Stub 区域、NSSA 区域和 Totally NSSA 区域将在下节介绍。

（5）Type5 LSA：自治系统外部 LSA（Autonomous system external LSA）

自治系统外部 LSA 由 ASBR 产生，描述到达 AS 外部的路由，**也仅可向普通区域中泛洪，**不能进入 Stub 区域、Totally Stub 区域、NSSA 区域和 Totally NSSA 区域。

（6）Type7 LSA：NSSA 外部 LSA（NSSA External LSA）

NSSA 外部 LSA 也由 ASBR 产生，内容几乎和 Type5 LSA 是相同的，**但它专用于 NSSA 区域和 Totally NSSA 区域连接的 ASBR 向 NSSA 区域内泛洪外部 AS 的路由，**然后经过 NSSA 区域 ABR 上转换成 Type5 LSA 向 OSPF 路由域内其他区域中传播。

（7）Type9/Type10/Type11 LSA：Opaque LSA

Opaque LSA 是一个被提议的 LSA 类别，是在标准的 LSA 头部后面加上特殊应用的信息组成，可以直接由 OSPF 协议使用，或者由其他应用分发信息到整个 OSPF 域间接使用。Opaque LSA 分为 Type9、Type10、Type11 三种类型，但它们各自可泛洪的区域不同：其中，Type9 LSA 仅在接口所在网段范围内传播，Type10 LSA 在区域内传播，Type11 LSA 在自治系统内传播。

【经验之谈】在 OSPF 中主要用到的就是 Type1～Type5 和 Type7 这 6 种 LSA。下面介绍在整个 OSPF 路由域中各区域中的设备是如何获取路由信息的。

① 在区域内部各路由器设备通过 Type1 LSA 来获取彼此的路由信息，实现相互路由通信。

② 在广播类型网络中，区域内非 DR、非 BDR 路由器与 DR、BDR 路由器之间是通过 Type2 LSA 获取路由信息的，实现非 DR、非 BDR 路由器与 DR、BDR 路由器之间的路由通信；各非 DR、非 BDR 路由器之间不相互获取路由信息，需全部通过 DR 或者 BDR，以及该区域的 ABR 与其他区域进行通信。

③ 在区域内部路由器与区域 ABR 之间，通过所在区域的 ABR 以 Type3 LSA 向内发布本区域各网段聚合路由信息，实现区域内路由器与对应区域的 ABR 路由通信。

④ 在不同区域之间，通过各自区域的 ABR 以 Type3 LSA 向内、外发布的本区域和外部区域各网段聚合路由信息（中间还需要骨干区域进行 LSA 转发），实现不同区域的路由器间的路由通信。

⑤ 在区域内部路由器与外部 AS 之间，先通过各区域的 ABR 以 Type4 LSA 向内发

布到达 ASBR 的聚合路由信息实现与 ASBR 的路由通信，然后通过对应 ASBR 向普通区域内部发布的 Type5 LSA 或者向 NSSA 区域和 Totally NSSA 区域发布的 Type7 LSA 实现与外部 AS 的路由通信。

12.1.4 几种特殊的 OSPF 区域

在 OSPF 网络的区域中，除了本节要介绍的 Stub 区域、Totally Stub 区域、NSSA 区域和 Totally NSSA 区域外，**其他区域（包括下面要介绍的骨干区域）都称为普通区域。**

1. 骨干区域

骨干区域是普通区域中的一种特殊区域，它的区域号固定为 0.0.0.0，也即区域 0。另外，骨干区域是连续的，或者通过“虚连接”（Virtual Link）连接两个或多个分离的骨干区域，但这些分离的骨干区域的区域号一样，均为 0。同时，要求其他区域必须与骨干区域直接连接，或者通过“虚连接”虚拟连接。如图 12-3 所示，普通区域 2 没有与骨干区域 0 直接连接（中间隔了一个区域 1），这时就可以在区域 1 连接骨干区域 0 和普通区域 2 的两端 ABR 中配置“虚连接”。“虚连接”被认为是属于骨干区域（相当于骨干区域的延伸）的，在 OSPF 路由协议看来，虚连接两端的两个路由器被一个点对点的链路连在一起，这样原本没有与骨干区域连接的区域就变成直接连接的了，成为普通区域了。通过虚连接连接两个非连续的骨干区域 0 的方法一样。

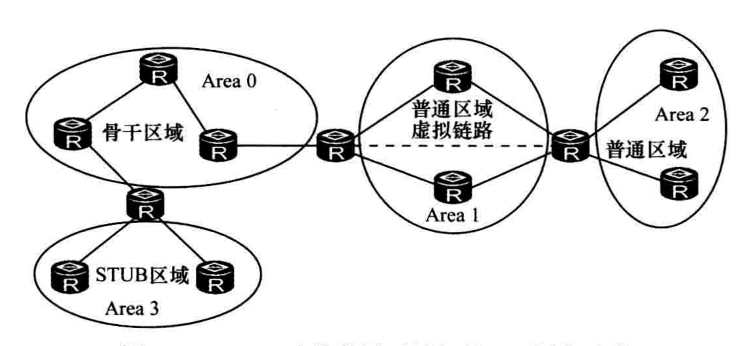


图 12-3 OSPF 中的普通区域与骨干区域的连接

骨干区域作为区域间通信传输和分布路由信息的中心，在一个 OSPF 路由域中，无论有没有划分区域，总是至少有一个骨干区域。区域间的通信先要被路由到骨干区域，然后再路由到目的区域，最后被路由到目的区域中的主机。在骨干区域中的路由器（都是 ABR）通告它们所连接的其他区域内的汇总路由到骨干区域中的其他路由器中。这些汇总通告在骨干区域内路由器传播，使得在骨干区域内部的每台路由器都有一个到达所连接的其他区域 ABR 的可用路由表。

2. Stub（末梢）区域

Stub 区域是一种专门为那些由性能较低的路由器组成、与 AS 外部没有太多路由通信的 AS 边缘区域简化区域内部路由器上的路由表而采取的一种优化措施。**只有处于 AS 边缘，且只有一个连接其他区域的 ABR，没有 ASBR，没有虚连接穿越的非骨干区域才可配置为 Stub 区域**，因为只有这样才能尽可能地减少区域内路由器的路由表项数量。

在 Stub 区域中是通过禁止与 AS 外部路由相关的 Type4 LSA 和 Type5 LSA 通过 ABR

进入区域内泛洪来实现的，仅允许同一 AS 中其他区域的 Type3 LSA 通过 ABR 进入区域泛洪。这样一来，在 Stub 区域内部路由器中**仅有 Type1 LSA、Type2 LSA（广播网络中才有）和 Type3 LSA 存在，没有 Type4 LSA 和 Type5 LSA**（更没有专用于 NSSA 和 Totally NSSA 区域的 Type7 LSA），可在一定程度上减小区域内部路由器上的路由表规模，减少设备内存资源消耗，提高路由效率。

在阻止了与 AS 外部相关的 Type4 LSA 和 Type5 LSA 进入区域后，也会带来一个问题，那就是 Stub 区域内部路由器不能获知外部 AS 的路由信息，不能与 AS 外部进行通信。但有时又的确需要与外部 AS 进行通信，于是新增了一条折衷的解决方法，就是**由 Stub 区域的 ABR 向本区域内部路由器泛洪一条指向自己的缺省路由（0.0.0.0）**，使 Stub 区域 ABR 作为区域内部路由器与外部 AS 通信的唯一出口。

【经验之谈】当一个 OSPF 的区域只存在一个区域出口点（只与一个其他区域连接）时，我们可以将该区域配置成一个 Stub 区域。这时，该区域的 ABR 会对区域内通告缺省路由信息。需要注意的是，一个 Stub 区域中的所有路由器都必须知道自身属于该区域（也就是需要在其中的路由器启用这项功能），否则 Stub 区域的设置不会起作用。下面的其他特殊区域配置也一样。

3. Totally Stub 区域

Totally Stub（完全末梢）区域从其名称就可以看出，它是相对前面介绍的 Stub 区域的变形版本，也是为那些设备性能相当低的边缘区域而设计的，可以进一步减少区域内路由器的路由表项。Totally Stub 区域所需满足的条件与 Stub 区域一样，**即只有处于 AS 边缘，且只有一个连接其他区域的 ABR，没有 ASBR，没有虚连接穿越的非骨干区域才可配置为 Totally Stub 区域**。

但在 LSA 的限制上，Totally Stub 区域比 Stub 区域更加严格，除了不允许与 AS 外部路由相关的 Type4 LSA 和 Type5 LSA 进入区域内外，**还不允许同一 AS 中其他区域的 Type3 LSA 经由 ABR 向区域内部路由器泛洪**。这样一来，在 Totally Stub 区域内部路由器中**仅有 Type1 LSA 和 Type2 LSA（广播网络中才有），没有 Type3 LSA、Type4 LSA 和 Type5 LSA**（同样更没有 Type7 LSA），可进一步大大减小区域内部路由器的路由表规模，进一步降低设备内在资源消耗，提高路由效率，这对那些较低配置的设备来说非常重要。

与 Stub 区域类似，为了解决有时 Totally Stub 区域内部路由器需要与其他区域，或者与 AS 外部进行通信的问题，也是由其 ABR 向区域内泛洪一条缺省路由，使得 Totally Stub 区域的 ABR 作为区域内部路由器与其他区域，或者与 AS 外部通信的唯一出口。

4. NSSA 区域

Stub 区域虽然为合理地规划网络描绘了美好的前景，但在实际的组网中利用率并不高（Stub 区域一般只存在于网络边缘），未免遗憾。但此时的 OSPF 协议已经基本成型，不可能再作大的修改。为了弥补缺陷，协议设计者提出了一种新的概念 NSSA（Not-So-Stubby Area，非纯末梢区域），并且作为 OSPF 协议的一种扩展属性单独在 RFC 1587 中描述。

NSSA 区域可以说是对原来的 Stub 区域概念的延伸，或者说是 Stub 区域修订版本，在必备条件方面有所放宽，即 **NSSA 区域可以位于非边缘区域，可以有多个 ABR（Stub**

区域仅允许有一个 ABR），可以有一个或多个 ASBR（Stub 区域中不允许有 ASBR）。在 LSA 的限制方面，NSSA 区域与 Stub 区域既有相同的地方，也有不同的地方，毕竟 NSSA 区域允许有 ASBR，且可以有多个 ABR。具体表现如下。

① **允许从其直接连接的 ASBR 上引入的 AS 外部路由以 Type7 LSA 进入 NSSA 区域中泛洪，然后在 ABR 上转换成 Type5 LSA 后以自己的身份发布到区域之外**，因为 Type7 LSA 是专门为 NSSA 区域新定义的，非 NSSA 区域设备不可识别。

② 与 Stub 区域一样，**允许区域间的 Type3 LSA 进入区域内部泛洪，不允许与其他区域中 ASBR 连接的 AS 外部路由相关的 Type4 LSA 和 Type5 LSA 进入 NSSA 区域内泛洪**。

从以上可以看出，NSSA 区域也限制了由其他区域中的 ASBR 所引入的 AS 外部路由进入区域内，但同样 NSSA 区域内部路由器有可能需要与其他区域连接的外部 AS 进行通信。为了解决这一问题，NSSA 区域仍采用缺省路由的方式来解决，就是在该区域的其中一个 ASBR 上（**NSSA 区域中可以有多个 ASBR**）向区域内部路由器泛洪一条指向自己的缺省路由，使该 ABR 作为区域内部路由器与其他区域所连接的外部 AS 进行通信的唯一路由。

通过以上介绍可以看出，**在 NSSA 区域中存在 Type1 LSA、Type2 LSA（广播网络中才有）、Type3 LSA 和 Type7 LSA，但没有 Type4 LSA 和 Type5 LSA**。

5. Totally NSSA 区域

Totally NSSA 区域可以说是前面介绍的 Totally Stub 区域和 NSSA 区域的结合体，具有它们双方的特点，具体表现如下。

① **与 NSSA 区域一样，可以位于非边缘区域，可以有多个 ABR 和 ASBR。**

② **与 NSSA 区域一样，允许区域中 ASBR 引入的 AS 外部路由以 Type7 LSA 进入区域内部泛洪**，然后经由该区域内的 ABR 将转换成 Type5 LSA 向 OSPF 路由域中其他所有区域进行发布。但不允许其他区域中的 ASBR 引入的路由进入区域内部，即**不允许 Type4 LSA 和 Type5 LSA 进入区域内部泛洪**。

③ **与 Totally Stub 区域一样，不允许 Type3 LSA 进入区域内部泛洪**（NSSA 区域是允许的），这样可进一步减少区域内部路由器的路由表规模。

同样，因为 Totally NSSA 区域禁止了其他区域的 Type3 LSA 和其他区域中 ASBR 连接的外部 AS 相关 Type4 LSA、Type5 LSA 进入区域内，所以使得区域内部路由器无法获知到达这些地方的路由信息。为了解决这一问题，Totally NSSA 区域也采用缺省路由的方式，就是在区域中选择一个 ABR 和 ASBR，在其中配置一条指向自己的缺省路由，然后在 Totally NSSA 区域内泛洪，使该 ABR 或 ASBR 作为区域内部路由器与其他区域或者其他区域中连接的外部 AS 进行通信的唯一出口。

以上 4 类特殊区域的异同如表 12-1 所示。

表 12-1　4 种特殊区域的比较

特点	Stub 区域	Totally Stub 区域	NSSA 区域	Totally NSSA 区域
是否必须位于 AS 边缘	是	是	不是	不是
ABR 数量	一个	一个	一个或多个	一个或多个

（续表）

特点	Stub 区域	Totally Stub 区域	NSSA 区域	Totally NSSA 区域
是否允许有 ASBR	不允许	不允许	允许一个或多个	允许一个或多个
是否允许虚连接穿过	不允许	不允许	不允许	不允许
Type3 LSA	允许	不允许	允许	不允许
Type4 LSA 和 Type5 LSA	不允许	不允许	不允许	不允许
Type7 LSA	不允许	不允许	允许	允许
缺省路由	作为区域内部路由器与 **AS 外部**通信时在到达 ABR 前的唯一路由，也作为**外部 AS** 与区域内部路由器通信时在到达 ABR 后的唯一路由	作为区域内部路由器与**其他区域、AS 外部**通信时在到达 ABR 前的唯一路由，也作为**其他区域、外部 AS** 与区域内部路由器通信时在到达 ABR 后的唯一路由	作为区域内部路由器与**其他区域 ASBR 连接的 AS 外部**通信时在到达 ABR 前的唯一路由，也作为**其他区域 ASBR 连接的外部 AS** 与区域内部路由器通信时在到达 ABR 后的唯一路由	作为区域内部路由器与**其他区域、其他区域 ASBR 连接的 AS 外部**通信时在到达 ABR 前或者 ASBR 的唯一路由，也作为**其他区域、其他区域 ASBR 连接的外部 AS** 与区域内部路由器通信时在到达 ABR 或者 ASBR 后的唯一路由
允许的 LSA	Type1 LSA、Type2 LSA 和 Type3 LSA	Type1 LSA 和 Type2 LSA	Type1 LSA、Type2 LSA、Type3 LSA 和 Type7 LSA	Type1 LSA、Type2 LSA 和 Type7 LSA
不允许的 LSA	Type4 LSA、Type5 LSA 和 Type7 LSA	Type3 LSA、Type4 LSA、Type5 LSA 和 Type7 LSA	Type4 LSA 和 Type5 LSA	Type3 LSA、Type4 LSA 和 Type5 LSA

12.1.5　OSPF 的网络类型

OSPF 协议支持多种不同类型的网络，当然必须都是运行 IP 协议的。根据链路层协议类型的不同将这些可支持的网络分为下列 4 种类型（**不同类型网络的报文发送方式不一样**）。

1. 广播（Broadcast）类型

当链路层协议是 Ethernet、FDDI 时，OSPF 缺省网络类型是广播（Broadcast）类型。在这种网络中，OSPF 的各种报文发送方式如下（有关 OSPF 的各种报文格式将在 12.2 节介绍）。

① 以组播形式（224.0.0.5，是运行 OSPF 设备的预留 IP 组播地址）发送 Hello 报文及所有源自 DR（指定路由器）的选举报文（有关 DR 和 BDR 选举将在 12.3.3 小节介绍）。

② 以组播形式（224.0.0.6，是 OSPF DR 的预留 IP 组播地址）向 DR 发送 LSU（链路状态更新）报文，然后 DR 将该 LSU 报文发送到 224.0.0.5。

③ 以单播形式发送 DD（数据库描述）报文、LSR（链路状态请求）报文和所有重传报文。

④ 正常情况下，以组播形式（224.0.0.5）发送 LSAck（链路状态应答）报文。当设备收到重复的 LSA 或达到最大生存时间的 LSA 被删除时，LSAck 以单播形式发送。

2. NBMA（Non-Broadcast Multi-Access）类型

当链路层协议是帧中继、X.25 时，OSPF 缺省网络类型是 NBMA。在该类型的网络中，以单播形式发送协议报文（Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文）。

3. 点到多点（point-to-multipoint，P2MP）类型

因为链路层协议中没有 Point-to-Multipoint 的概念，所以 P2MP 必须是由其他的网络类型强制更改的。在该类型的网络中，以组播形式（224.0.0.5）发送 Hello 报文，以单播形式发送 DD 报文、LSR 报文、LSU 报文、LSAck 报文。

4. 点到点 P2P（point-to-point）类型

当链路层协议是 PPP、HDLC 和 LAPB 时，OSPF 缺省网络类型是 P2P。在该类型的网络中，以组播形式（224.0.0.5）发送各种 OSPF 协议报文。

以上 4 种网络类型的特点及缺省选择如表 12-2 所示。

表 12-2 OSPF 的网络类型特点及缺省选择

网络类型	特点	缺省选择
广播类型（Broadcast）	通常以组播形式发送 Hello 报文、LSU 报文和 LSAck 报文，以单播形式发送 DD 报文和 LSR 报文	当链路层协议是 Ethernet、FDDI 时，缺省情况下 OSPF 认为网络类型是 Broadcast
NBMA 类型	以单播形式发送 Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文。NBMA 网络必须是全连通的，即网络中任意两台路由器之间都必须直接可达	当链路层协议是 ATM 时，缺省情况下 OSPF 认为网络类型是 NBMA
P2P 类型	以组播形式发送 Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文	当链路层协议是 PPP、HDLC 和 LAPB 时，缺省情况下 OSPF 认为网络类型是 P2P
P2MP 类型	以组播形式发送 Hello 报文，以单播形式发送 DD 报文、LSR 报文、LSU 报文、LSAck 报文。P2MP 网络中的掩码长度必须一致	没有一种链路层协议会被缺省为是 P2MP 类型，必须是由其他的网络类型强制更改的

12.2 OSPF 报头及各种报文格式

OSPF 把自治系统划分成逻辑意义上的一个或多个区域，通过 LSA 的形式发布路由信息，然后依靠在 OSPF 区域内各设备间各种 OSPF 报文的交互来达到区域内路由信息的统一，最终在区域内部路由器中构建成完全同步的 LSDB。因为 OSPF 是专为 TCP/IP 网络而设计的路由协议，所以 OSPF 的各种报文是封装在 IP 报文内的，可以采用单播或组播的形式发送。

12.2.1 OSPF 协议报头格式

OSPF 报文主要有 5 种：Hello 报文、DD（Database Description，数据库描述）报文、LSR（LinkState Request，链路状态请求）报文、LSU（LinkState Update，链路状态更新）报文和 LSAck（LinkState Acknowledgment，链路状态应答）报文。它们使用相同的 OSPF

报头格式（均以 OSPFv2 版本为例进行介绍），如图 12-4 所示。

1	1	2 (bytes)
Version	Packet Type	Packet Length
Router ID		
Area ID		
Checksum		AuType
Authentication		

图 12-4　OSPF 协议报头格式

① Version：版本字段，占 1 个字节，指出所采用的 OSPF 协议版本号，OSPFv2 的版本值就为 2，即 0000 0010。

② Packet Type：报文类型字段，标识对应报文的类型，取值为 1～5 的整数，分别对应前面说的 Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文这 5 种 OSPF 报文。这些报文的具体格式将在下面各小节介绍。

③ Packet Length：包长度字段，占 2 个字节，标识整个报文（包括 OSPF 报头部分和后面各报文内容部分）的字节长度。

④ Router ID：路由器 ID 字段，占 4 个字节，指定发送报文的源路由器 ID。

⑤ Area ID：区域 ID 字段，占 4 个字节，指定发送报文的路由器接口所在的 OSPF 区域号。

⑥ Checksum：校验和字段，占 2 个字节，是对整个报文（包括 OSPF 报头和各报文具体内容，但不包括下面的 Authentication 字段）的校验和，用于**对端路由器**校验报文的完整性和正确性。

⑦ AuType：验证类型字段，占 2 个字节，指定在进行 OSPF 报文交互时所需采用的验证类型，0 为不验证，1 为进行简单验证，2 为采用 MD5 方式验证。

⑧ Authentication：验证字段，占 8 个字节，具体值根据不同验证类型而定。验证类型为不验证时，此字段没有数据；验证类型为简单验证时，此字段为验证密码；验证类型为 MD5 验证时，此字段为 MD5 摘要消息。

12.2.2　OSPF Hello 报文及格式

OSPF 协议使用一种称之为 Hello 的报文来建立和维护相邻邻居路由器之间的邻接关系。这个报文很简单，容量也很小，仅用来向邻居路由器证明自己的存在，就像人与人之间打招呼一样。第 11 章中已经介绍过，RIP 邻居路由器之间的邻居关系建立和路由更新都是通过发送 Hello 报文进行的。显然 OSPF 的这种 Hello 报文更简单，可大大减小网络中的报文传输流量。

在 P2P 和广播类型网络中，Hello 报文是以 HelloInterval 为周期（缺省为 10 s），**以组播方式**向 224.0.0.5 组播组发送一次；但在 P2MP 和 NBMA 类型网络中，OSPF 路由器是以 PollInterval 为周期（缺省为 60 s），**以单播方式向状态为 Down 的邻居**发送一个 Hello 报文（其他类型的网络是不会把 Hello 报文发送给状态为 Down 的路由器的）。如果在设

定的 DeadInterval 时间（**通常至少是 Hello 报文发送时间间隔的 4 倍**）内没有收到对方 OSPF 路由器发送来的 Hello 报文，则本地路由器会认为该对方路由器无效。

Hello 报文内容包括一些定时器设置、DR、BDR 以及本路由器已知的邻居路由器。整个 Hello 报文格式如图 12-5 所示，上部分为图 12-4 所示的 OSPF 报头部分，下部分为 Hello 报文内容部分。Hello 报文内容部分各字段说明如表 12-3 所示。

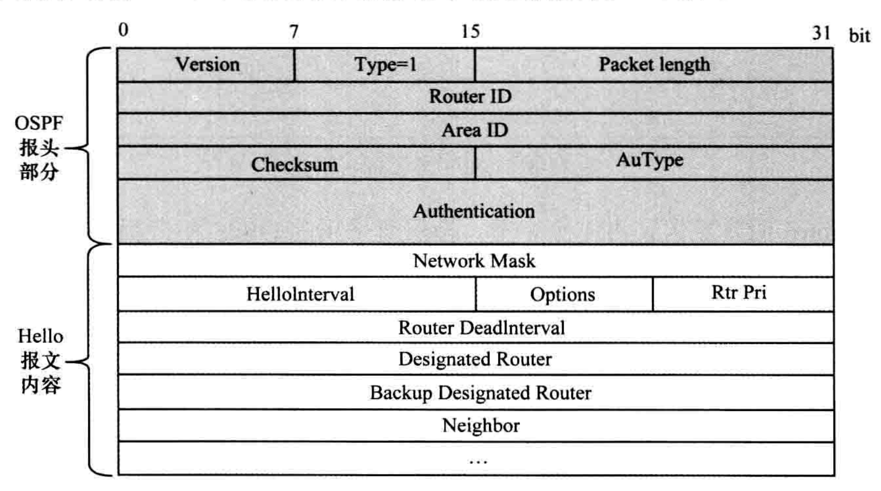


图 12-5 Hello 报文格式

表 12-3 Hello 报文内容部分字段说明

字段名	长度	功能
Network Mask	4 字节	发送 Hello 报文接口的 IP 地址所对应的子网掩码
HelloInterval	2 字节	指定发送 Hello 报文的时间间隔，缺省为 10 s
Options	1 字节	可选项，置“1”时代表具有相应特性，置“0”时代表不具备相应特性，包括 E：是否允许泛洪 AS-external-LAS；MC：是否允许转发 IP 组播报文；N：是否允许处理 Type 7 LSA; DC：是否允许处理按需链路
Rtr Pri	1 字节	指定本路由器的 DR 优先级值，缺省为 1。如果设为 0，则表示本路由器不参与 DR/BDR 选举
RouterDeadInterval	4 字节	指定检测本地路由器失效的时间，缺省为 40 s。指示当收到此 Hello 报文的路由器在此时间内没有收到本路由器再次发来的 Hello 报文，则认为本路由器已失效
Designated Router	4 字节	指定 DR 的接口 IP 地址
Backup Designated Router	4 字节	指定 BDR 的接口 IP 地址
Neighbor	4 字节	指定邻居路由器的路由器 ID。图 12-5 最下面的省略号（…）表示可以指定多个邻居路由器 RID

从表中可以看出，在 OSPF 路由器上可以配置 Hello 报文的发送时间间隔（是基于接口来配置的），具体将在本章后面介绍。

12.2.3 OSPF DD 报文及格式

DD 报文用来描述本地路由器的链路状态数据库（LSDB），即在本地 LSDB 中包括哪些 LSA。在两个 OSPF 路由器初始化连接时要交换 DD 报文，以便进行数据库同步。

DD 报文内容部分包括 DD 报文序列号和 LSDB 中每一条 LSA 的头部等，如图 12-6 所示，对应的各字段说明如表 12-4 所示。对端路由器根据所收到的 DD 报文中的 OSPF 报头就可以判断出是否已有这条 LSA。由于数据库的内容可能相当长，所以可能需要多个 DD 报文的交互来完成双方 LSDB 的同步。所以有三个专门用于标识 DD 报文序列的比特位，即 DD 报文格式中的 I、M 和 M/S 这三位。接收方对接收到的连续 DD 报文重新排序，使其能还原所接收的 DD 报文。

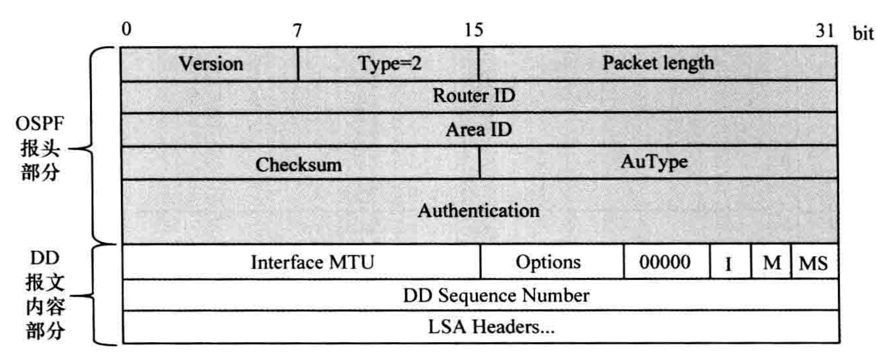


图 12-6　DD 报文格式

表 12-4　DD 报文内容部分字段说明

字段名	长度	功能
Interface MTU	2 字节	指出发送 DD 报文的接口在不分段的情况下，可以发出的最大 IP 报文长度
Options	1 字节	可选项，置“1”时代表具有相应特性，置“0”时代表不具备相应特性，包括 E：是否允许泛洪 AS-external-LAS；MC：是否允许转发 IP 组播报文；N：是否允许处理 Type 7 LSA；DC：是否允许处理按需链路
I	1 比特	指定在连续发送多个 DD 报文，如果是第一个 DD 报文则置 1，其他的均置 0
M	1 比特	指定在连续发送多个 DD 报文，如果是最后一个 DD 报文则置 0，否则均置 1
M/S	1 比特	设置进行 DD 报文双方的主从关系，如果本端是 Master（主）角色，则置 1，Slave（从）角色置 0
DD Sequence Number	4 字节	指定所发送的 DD 报文序列号。主从双方利用主端设备的 DD 报文序列号来确保 DD 报文传输的可靠性和完整性
LSA Header	4 字节	指定 DD 报文中所包括的 LSA 头部。后面的省略号（…）表示可以指定多个 LSA 头部

DD 交换过程按询问/应答方式进行，在 DD 报文交换中，一台为 Master（主）角色，另一台为 Slave（从）角色。Master 路由器向 Slave 路由器发送它的路由表内容，并规定起始序列号，每发送一个 DD 报文，序列号加 1，Slave 路由器则使用 Master 路由器的序列号进行确定应答。但是显然，主、从之间的关系会因每个 DD 交换的不同而不同，因为双方可能都有对方没有的 LSA，网络中的所有路由器会在不同时刻担当不同的角色。

12.2.4　OSPF LSR 报文及格式

LSR 报文用于请求相邻路由器链路状态数据库中的一部分数据。当两台路由器互相

交换完 DD 报文后，知道对端路由器有哪些 LSA 是本 LSDB 所没有的以及哪些 LSA 是已经失效的，则需要发送一个 LSR 报文，向对方请求所需的 LSA。

LSR 报文内容包括所需的 LSA 摘要，具体格式如图 12-7 所示，LSR 报文内容部分各字段说明如表 12-5 所示。

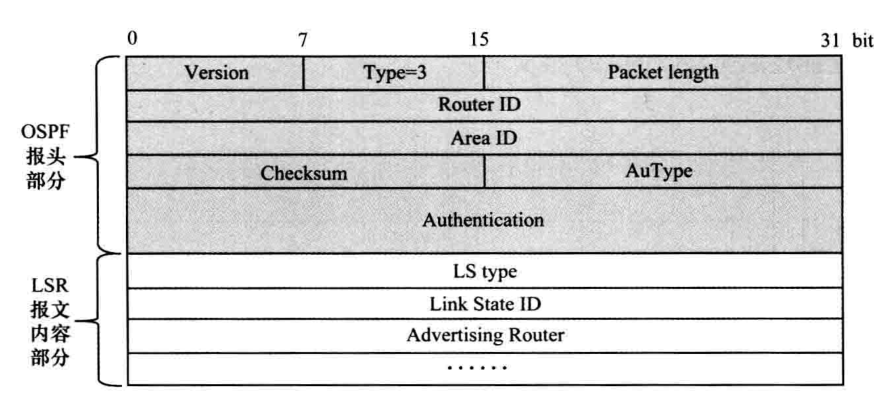


图 12-7 LSR 报文格式

表 12-5 LSR 报文内容部分字段说明

字段名	长度	功能
LS type	4 字节	指定所请求的 LSA 类型，主要有 7 类，具体参见 12.1.3 小节
Link State ID	4 字节	用于指定 ospf 所描述的部分区域，该字段的使用方法根据 LSA 类型不同而不同：当为 Type1 LSA 时，该字段值是产生该 LSA 的路由器的 Router-ID；当为 Type2 LSA 时，该字段值是 DR 的接口地址；当为 Type3 LSA 时，该字段值是目的网络的网络地址，当为 Type4 LSA 时，该字段值是 ASBR 的 Router-ID；当为 Type5 LSA 和 Type7 LSA 时，该字段值是目的网络的网络地址
Advertising Router	4 字节	指定产生此 LSR 报文的路由器 ID

12.2.5 OSPF LSU 报文及格式

LSU 报文是 LSR 请求报文的应答报文，用来向对端路由器发送所需的真正 LSA 内容，可以是多条 LSA 完整内容的集合。LSU 报文内容部分包括此次一共发送的 LSA 数量和每条 LSA 的完整内容，如图 12-8 所示，报文内容部分的两个字段如表 12-6 所示。

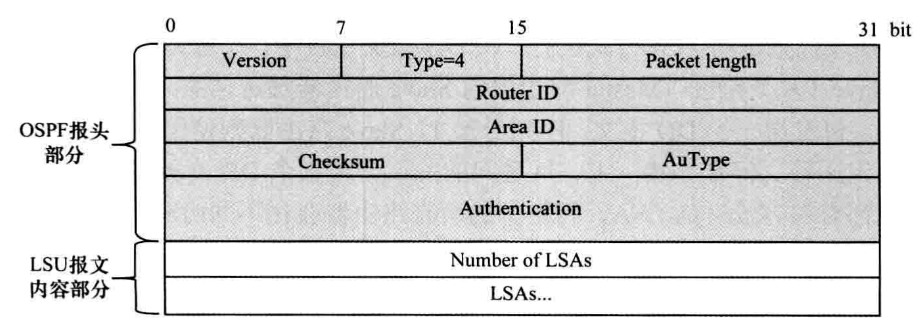


图 12-8 LSU 报文格式

有关 LSA 的类型参见 12.1.3 小节。LSU 报文在支持组播和多路访问的链路上是以组播方式将 LSA 泛洪出去的，并且对没有收到对方确认应答（就是下面将要介绍的 LSAck 报文）的 LSA 进行重传，但重传时的 LSA 是直接送到没有收到确认应答的邻居路由器上，而不再是泛洪。

表 12-6　　LSU 报文内容部分字段说明

字段名	长度	功能
Number of LSA	4 字节	指定此报文中共发送的 LSA 数量
LSAs	4 字节	是一条条具体的 LSA 完整信息，后面的省略号表示可多条 LSA

12.2.6 OSPF LSAck 报文及格式

LSAck 报文是路由器在收到对端发来的 LSU 报文后发出的确认报文，内容是需要确认的 LSA 头部（LSA Headers）。LSAck 报文根据不同链路以单播或组播形式发送，具体参见 12.1.5 小节的说明。整个 LSAck 报文的格式如图 12-9 所示，LSA 报头格式如图 12-10 所示，各字段具体说明如表 12-7 所示。

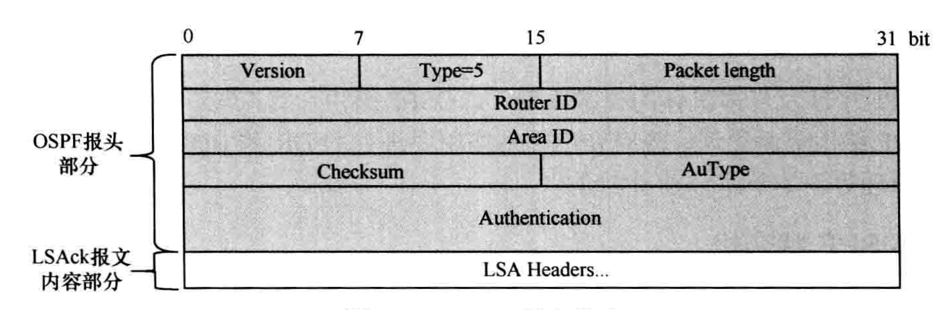


图 12-9　LSAck 报文格式

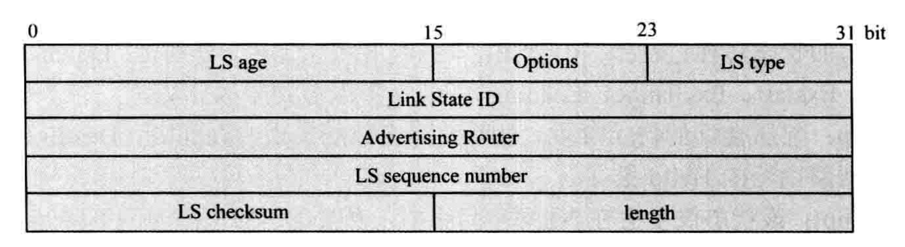


图 12-10　LSA 报头格式

表 12-7　　LSA 报头字段说明

字段名	长度	功能
LS age	2 字节	LSA 产生后所经过的时间，以秒为单位。LSA 在本路由器的链路状态数据库（LSDB）中会随时间老化，当泛洪扩散时，路由器会把 LSA 的老化时间增加一个 Trans-delay 的秒数
Options	1 字节	可选项，置“1”时代表具有相应特性，置“0”时代表不具备相应特性，包括 E：是否允许泛洪 AS-external-LAS；MC：是否允许转发 IP 组播报文；N：是否允许处理 Type 7 LSA；DC：是否允许处理按需链路

（续表）

字段名	长度	功能
LS type	1 字节	对应 LSA 的类型，Type1～Type5 LSA 的取值分别为 1～5 的整数，这些 LSA 类型的具体说明参见 12.1.3 小节
Link State ID	4 字节	链路状态 ID，但不同类型的 LSA 该字段的定义不一样：Type1 LSA 为产生此 LSA 的路由器的 Router ID，Type2 LSA 为 DR 的 IP 地址，Type3 LSA 为所通告的区域外的网络地址，Type4 LSA 为所通告区域外的 ASBR 的 Router ID，Type5 LSA 和 Type7 LSA 为所要通告的外部 AS 的网络地址
Advertising Router	4 字节	始发对应 LSA 的路由器的 ID
LS sequence number	4 字节	对应 LSA 的序列号，其他路由器根据这个值可以判断哪个 LSA 是最新的
LS checksum	2 字节	是对除了 LS age 字段外 LSA 报头的全部信息的校验和
length	2 字节	LSA 报头的总长度，以字节为单位

12.3 OSPF 工作原理

在 OSPF 中涉及许多具体的技术原理，如 OSPF 路由计算原理、OSPF 区域间的路由原理、OSPF 路由更新原理，还有在广播网络中要进行的 DR 和 BDR 选举以及 OSPF 报文的验证原理等，本节将分别予以介绍。

12.3.1 OSPF 状态机

OSPF 是一种链路状态路由协议，邻居设备间交换的是链路状态信息，OSPF 路由也是依据由链路状态信息构成的链路状态数据库（LSDB）形成的。所以在 OSPF 中，建立设备间的邻居关系，交换彼此的 LSDB 就显得格外重要了。而邻居关系建立的流程体现在 OSPF 接口的状态转换过程中。在 OSPF 中共有 8 种状态机，分别是：Down、Attempt、Init、2-way、Exstart、Exchange、Loading、Full，下面分别予以介绍。

① Down：邻居会话的初始阶段，表明没有在邻居失效时间间隔（DeadInterval）内收到来自邻居路由器的 Hello 报文。

② Attempt：**该状态仅发生在 NBMA 网络中**，表明在邻居失效时间间隔超时后仍然没有对端发来的 Hello 应答报文。此时路由器依然会以轮询 Hello 报文发送时间间隔（PollInterval）向对端发送 Hello 报文。

③ Init：收到不包含自己路由器 ID 的 Hello 报文后状态转换为 Init。

④ 2-way：收到包含有自己的路由器 ID 的 Hello 报文后则状态转换为 2-way。

⑤ Exstart：在进行 DR、BDR 选举后形成邻居关系，则从 Init 状态转换到 Exstart 状态，通过不带 LSA Header 字段内容的 DD 报文协商主、从关系，并确定 DD 报文的序列号。

⑥ Exchange：主、从关系协商完毕后，主设备开始向从设备正式发送带有 LSA Header 字段内容的 DD 报文，此时双方状态转换为 Exchange。

⑦ Loading：DD 报文交换完成后从设备状态转换为 Loading。此时，通信双方可以 LSR 报文向对方请求 LSA 更新，而以 LSU 报文对对方请求进行应答。

⑧ Full：当设备收到对端发来的，由自己所请求的 LSA 报文后向对端发送 LSAck 报文，同时发给对端的 LSA 后也收到了来自对端的 LSAck 报文，之后，则本地设备自动切换为 Full 状态了。

以上这些 OSPF 状态机应用于 OSPF 邻接关系的建立，具体的转换流程将在下节介绍。

12.3.2　OSPF 邻接关系建立流程

OSPF 邻居关系的建立和维持都是依靠 Hello 报文交互来实现的，而 OSPF 邻接关系的建立则需要一个比较复杂的流程，也是邻居设备接口的状态机转换过程。

整个 OSPF 设备间邻接关系的建立过程分为 4 个主要阶段：**邻居发现阶段、主从关系确立阶段、数据库同步阶段、完全邻接阶段**。这 4 个阶段中每个阶段都包含一种或者多种状态机的转换。初始状态下，所有 OSPF 接口的邻居状态均为 Down 状态，表明没有与任何设备建立邻居关系，更没有与任何设备建立邻接关系（**邻居关系不等于邻接关系**）。

下面仅以 P2P 和广播类型网络中的两台 OSPF 路由器为例介绍建立双向邻接关系的流程，以及对应的 OSPF 状态机迁移过程（假设 R1 路由器先启动了 OSPF 进程），具体如图 12-11 所示。

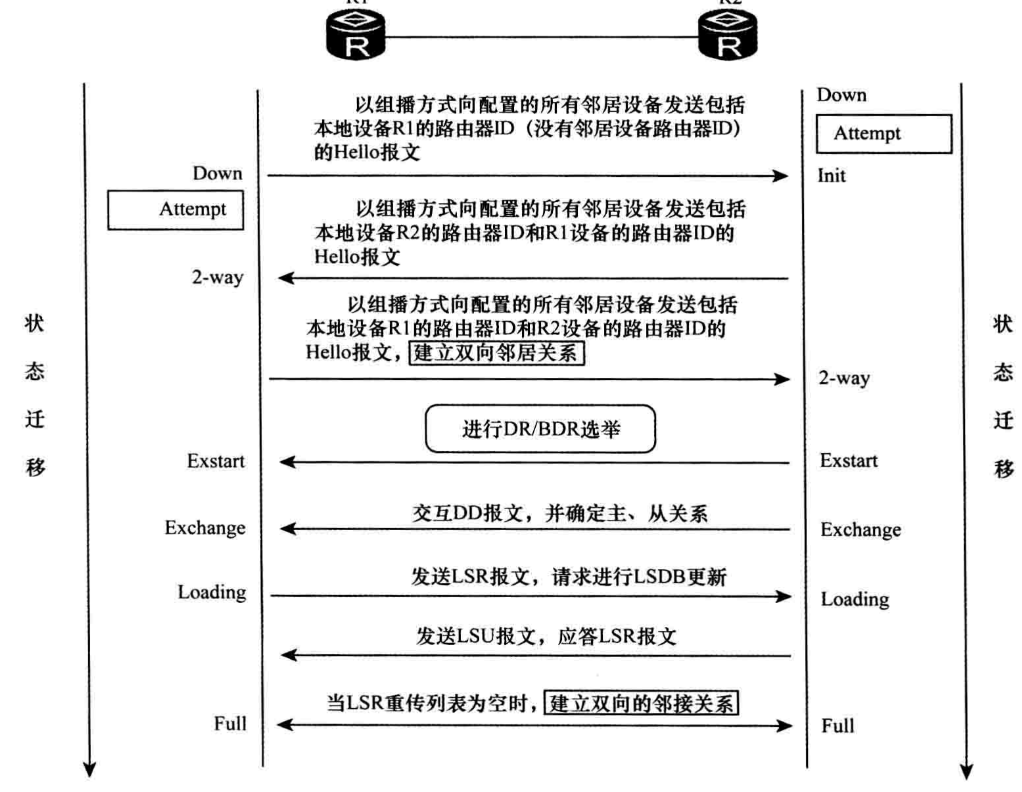


图 12-11　OSPF 邻接关系建立流程

1. 邻居发现阶段

① 首先，当 R1 的 OSPF 接口启动路由进程后，会以组播方式（目的地址为组播地址 224.0.0.5）向所连接的同网段所有直接连接的 OSPF 设备发送一个 Hello 报文。此时，因为 R1 还没有与其他任何设备建立邻居关系，不知道其他设备的路由器 ID，所以在此 Hello 报文的 Router ID 字段中仅封装了本地 OSPF 路由器的路由器 ID，在 Neighbor 字段中没有封装任何路由器 ID。有关 Hello 报文的结构参见 12.2.2 小节。

② 当 R2 收到来自 R1 的 Hello 报文后，**将接收来自 R1 的 Hello 报文的接口转换成 Init 状态**。同时 R2 从接收到的 Hello 报文中获取 R1 的路由器 ID，添加到邻居列表中。然后在 DeadInterval 超时前，以组播方式向所连接的网段中的所有直接连接的 OSPF 设备发送一个在 Router ID 字段中封装本地设备 R2 的路由器 ID，在 Neighbor 字段中封装 R1 的路由器 ID 的 Hello 报文。

③ 当 R1 收到来自 R2 的 Hello 报文，且发现里面有自己的路由器 ID 后，**将接收来自 R2 的 Hello 报文的接口转换成 2-way 状态**，同时 R1 从接收到的 Hello 报文中获取 R2 的路由器 ID，添加到邻居列表中，然后在 DeadInterval 超时前，以组播方式向所连接的网段中的所有直接连接的 OSPF 设备发送一个在 Router ID 字段中封装本地设备 R1 的路由器 ID，在 Neighbor 字段中封装 R2 的路由器 ID 的 Hello 报文。

④ 当 R2 再次收到来自 R1 的 Hello 报文，且发现里面有自己的路由器 ID 后，**将接收来自 R1 的 Hello 报文的接口转换成 2-way 状态**。这时 R1 和 R2 就建立了双向的 2-way 邻居关系。

通过以上 4 步（其实是一个两次握手过程），R1 和 R2 间就建立起了邻居关系，进入主从关系确立阶段。

2. 主从关系确立阶段

① 在双方都进入 2-way 状态后，R1 和 R2 通过先前各自获取的 Hello 报文的信息进行 DR、BDR 选举，选举完成后双方都进入 **ExStart 状态**。

DR 和 BDR 是由同一网段中所有路由器根据路由器优先级和路由器 ID 选举出来的，只有 Hello 报文中 Rtr Pri（优先级）字段大于 0 的路由器才具有选举资格。具体的选举过程如下。

- 在与一个或多个邻居之间的双向通信建立起来之后，本地路由器对每个邻居发送来的 Hello 包中的优先级、DR 和 BDR 域进行检查。此时所有路由器都宣称自己为 DR（将它们自己的接口地址置于 Hello 包的 DR 字段中）；同时，所有路由器都宣称自己为 BDR（将它们自己的接口地址置于 Hello 包的 BDR 字段中）。
- 如果一或多个备选路由器将它（们）自身的接口地址置于 DR 字段中，拥有最高优先级的邻居将被宣告为 DR。如果路由器优先级一样，拥有最高路由器 ID 的邻居将被选举出来。
- 然后将自身的接口地址置于 BDR 字段中的路由器中选择拥有最高优先级的路由器作为 BDR。如果这些宣称自己为 BDR 路由器的优先级相等，则拥有最高路由器 ID 的邻居将被选举作为 BDR。
- 如果没有任何路由器被宣告为 BDR，则拥有最高优先级的非 DR 邻居路由器将被宣告为 BDR；如果有多个优先级相同的路由器，则拥有最高路由器 ID 的邻居将被选举作为 BDR。

② 进入 ExStart 状态后，双方路由器开始以 DD 报文进行交互，确定双方的主从关系，确定用于数据交换的初始的 DD 报文的序列号，以保证路由器得到的永远是最新的链路状态信息。

在开始交互时，R1 和 R2 双方都是在 M/S 字段设为 1（代表自己为主设备），在 DD Sequence Number 字段加上各自当前 DD 报文的序列号（每发送一次序列号加“1”），LSA Header 字段为空的 DD 报文进行交互的。最终会根据双方的路由器 ID 来确定双方的主从关系，路由器 ID 大的成为主设备（此处假设为 R2）。

确认好主从关系后，从设备 R1 以主设备 R2 的 DD 报文序列号向主设备发送 DD 报文，并且置 M/S 字段值设为 0（代表自己为从设备），同样里面的 LSA Header 字段为空，并转换自己接收 DD 报文的接口为 **Exchange 状态**。主设备 R2 在收到从设备 R1 的 DD 报文后也将自己接收 DD 报文的接口转换为 **Exchange 状态**。

通过以上两步，R1 和 R2 邻接关系建立流程进入了数据库同步阶段了。

3. 数据库同步阶段

① 主设备 R2 开始连续向从设备 R1 发送带有 LSA Header 字段的报文（其中第一个 DD 报文的 I 字段值为 1，代表为连续 DD 报文中的第一个报文，其余连续 DD 报文的 I 字段值均为 0），M 字段为 1（代表后面还有报文）对从设备 R1 进行数据库更新。但每发送一次 DD 报文，其序列号都要加“1”。从设备 R1 每次收到来自主设备 R2 的 DD 报文后均以收到的 DD 报文序列号进行响应（但里面的 LSA Header 字段为空）。

② 当主设备 R2 向从设备 R1 发送最后一个 DD 报文时，将 M 字段置为 0，代表为最后一个 DD 报文，同时 LSA Header 字段为空，并将接收 DD 报文的接口转换为 **Loading 状态**。当从设备 R1 收到主设备 R2 带有 M 字段为 0 的 DD 报文后便知道这是最后一个 DD 报文了，此时也将接收 DD 报文的接口转换为 **Loading 状态**。

③ 当主设备 R2 发送完 DD 报文后，从设备 R1 开始依据所接收的 DD 报文中的 LSA Header 字段检查自己的 LSDB，如果发现有些 LSA 在自己的 LSDB 中没有，则从设备 R1 会以 LSR 报文向主设备 R2 发出更新请求。当主设备 R2 收到 LSR 报文后会以 LSU 报文向从设备 R1 发送对应的 LSA。从设备 R1 在收到来自主设备 R2 的 LSU 报文后，会以 LSAck 报文进行确认。

说明　因为双方都可能有对方没有的 LSA，或者一方的 LSA 版本更新，所以在 DD 报文交互中，主从角色不是固定的，双方都可以向对方发送 LSR 报文请求更新。

通过以上两步完成了链路状态数据库的同步，进入最后的完全邻接阶段。最终实现同一区域中每台 OSPF 区域内部路由器的 LSDB 是完全一致的，实现了整个区域内的拓扑结构同步。

4. 完全邻接阶段

当双方的 LSDB 完全同步后，双方均**转为 Full 状态**，双方 OSPF 接口间正式建立了完全邻接的关系。

12.3.3 OSPF 路由计算基本过程

我们知道，OSPF 网络是在一个 AS 中以区域为单位的分层结构，而且在区域中又分

为两种不同角色：骨干区域和普通区域。这就决定了 OSPF 的路由也必定是分层的，分为区域内路由和区域间路由，而不是像 RIP 路由那样是扁平的。

整个 OSPF 路由计算过程是在 OSPF 设备间建立了完全的邻接关系后（也就是上节介绍的 4 个阶段）进行的，依据的就是路由器为所连接的各个区域所保存的 LSDB（每个连接区域都有一个专门的 LSDB）。但在具体的路由计算中，又分区域内路由和区域间路由两个方面，下面依次介绍。

1. OSPF 区域内路由计算

当网络重新稳定下来后，OSPF 路由器会根据其各自的 LSDB 采用 SPF（最短路径优先）算法（具体算法为 Dijkstra，IS-IS 路由也采用这种算法）独立地计算到达每一个目的网络的路径，并将路径存入路由表中。路由表中包含该路由器到每一个可到达目的地址、开销和下一跳（next-hop）。OSPF 区域内路由是由 OSPF 内部路由器使用最小开销的路径到达目的网络，且区域内的路由不被聚合。

OSPF 的 Dijkstra 算法是利用开销来计算路由路径性能的，开销最小者即为最短路径。在配置 OSPF 路由器时可根据实际情况，如链路带宽、时延等设置链路的开销大小。开销越小，则该链路被选为路由的可能性越大。这里的开销是根据链路类型来计算的，不同的链路类型对应的开销值不一样。下面，具体介绍 Dijkstra 算法原理。

在 Dijkstra 算法中，为了在一对给定的路由器节点之间选择一条最短（其实是指链路开销最小）路由路径，只需在通信子网拓扑图中找到在这起始和结束节点之间的中间节点串连起来后链路开销最短的路径即可。它把最短路由的节点标识为工作节点，并且是永久性的节点，其到达源节点的距离值是不能改变的，其他的标识为临时性的节点，其到达源节点的距离可能会随工作节点的不同而改变。所有工作节点串联起来就是对应源节点和目的节点之间的最短路由路径。

图 12-12 所示的子网图是一个典型的最短路径路由算法子网图，图中的每一个节点（以字母标注）代表一台 OSPF 路由器，每条线段代表一条通信链路，线段上的数字代表对应链路的开销值。现假设要使用 Dijkstra 算法计算节点 A 到节点 D 之间的最短路径。在网络中路由器启动时，首先需要初始化，测量每条链路的开销，参见图 12-12 各条线段上的数字。下面是从 A 节点到达 D 节点的路由确定步骤。

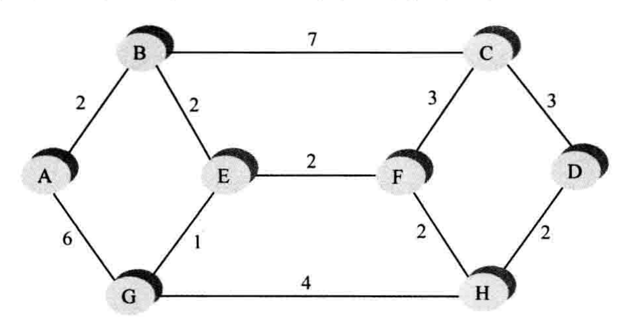


图 12-12 典型的 Dijkstra 算法子网图

① 首先将源节点 A 标记为永久性工作节点（用箭头来特别标识），然后依次检查每一个与 A 节点直接连接的相邻节点，并且把它们与 A 节点之间的距离重新以（*n*，*N*）的方式进行标识，其中的 *n* 为与 A 节点相距的链路开销，*N* 为最近的工作节点。

因为本示例中与节点 A 直接相邻的节点只有 B 和 G，所以仅需标识这两个节点与 A 节点之间距离。此时的工作节点为 A，如图 12-13 所示，B 节点的标识为（2，A），G 节点的标识为（6，A），因为 B 节点到 A 节点的链路开销为 2，G 节点到 A 节点的链路开销为 6。其他与 A 节点不相邻的节点的距离标识为无穷远。

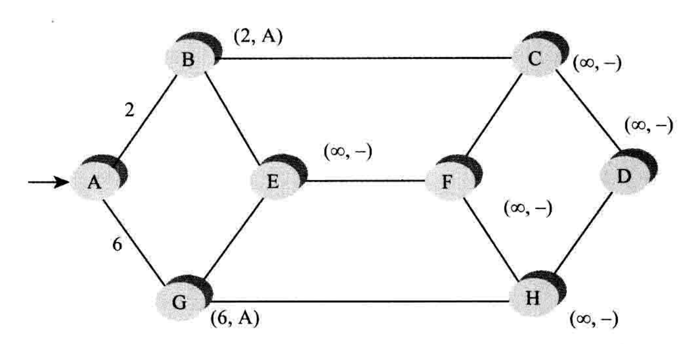


图 12-13　以 A 节点为工作节点标记其他相邻节点与 A 节点之间的距离

② 比较 B 和 G 这两个节点与 A 节点之间距离，可以看出 B 节点的距离更短，于是把 B 节点改为工作节点（箭头移到 B），同时变为永久性节点，其他节点（包括 G 节点）标注为临时节点。然后以 B 节点为工作节点，标记直接相邻的节点到源节点 A 的距离，当然对于前面已经计算过的节点将略过，如源节点 A 和 G 节点。

在本示例与 B 节点直接相邻的节点中，除了 A 节点外还有 C、E 这两个节点。C 节点到达 A 节点的距离就是 C 节点到 B 节点的链路开销 7，再加上 B 节点到 A 节点的链路开销 2，所以 C 节点到 A 节点的距离为 2+7=9，标识为（9，B）。同理，E 节点到 A 节点的距离为 2+2=4，标识为（4，B），如图 12-14 所示。其他既不与 A 节点，又不与 B 节点相邻的仍为无穷远。

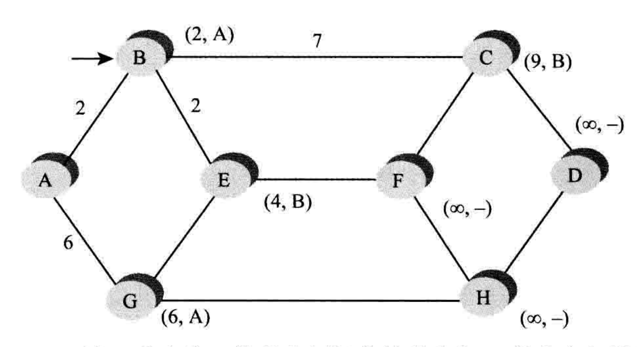


图 12-14　以 B 节点为工作节点标记其他节点与 A 节点之间的距离

③ 同样经过比较得出，E 节点到 A 节点之间的距离（为 4），比 C 节点到 A 节点的距离（为 9）近，所以此时把 E 节点改为工作节点（箭头移到 E），同时标注 E 节点为永久性节点，其他节点（包括 C 节点）标注为临时节点。

按同样方法标记与 E 节点直接相邻的节点（包括节点 B、节点 G 和节点 F）到 E 节点的距离，但对于前面已计算过的永久性 B 节点不再重新计算，而对于虽然原来已计算过，但为临时性节点的 G 以及 F 节点均需要重新计算。最终 G 节点的标识改为（5，E）

（在此步以前为（6，A）），F 节点标识为（6，E），表示 G 节点和 F 节点到达 A 节点的距离分别为 5 和 6，如图 12-15 所示。

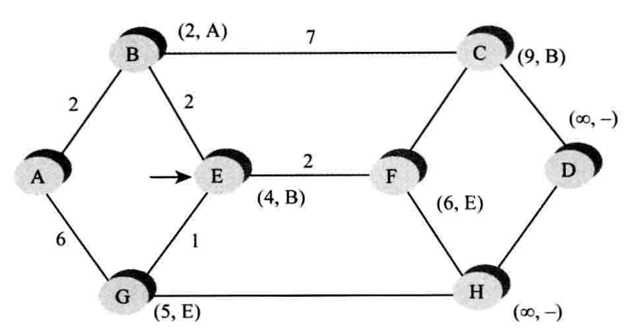


图 12-15 以 E 节点为工作节点标记其他节点与 A 节点之间的距离

④ 再用同样的方法比较 G 节点和 F 节点到达 A 节点之间的距离，可以得出 G 节点更近，所以此时把 G 节点改为工作节点（箭头移到 E），同时标注 G 节点为永久性节点，其他节点（包括 F 节点）标注为临时节点，如图 12-16 所示。

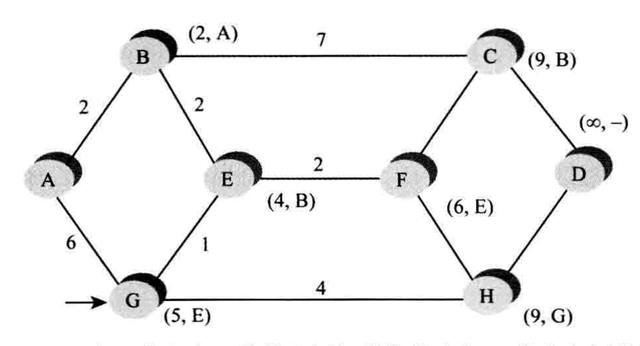


图 12-16 以 G 节点为工作节点标记其他节点与 A 节点之间的距离

再看一下与 G 节点直接相邻的节点，包括 A、E、H 这 3 个节点，但是 A、E 这两个节点在前面都已标识为永久性节点了，标识是不能更改的，所以在这里只需对 H 节点计算到达 A 节点的距离了。经过计算得出为（9，G）。

在这里就要出现问题了，按照上面的计算，此时应该把 H 节点标识为下一个工作节点，但事实上，由 H 节点经 G 节点到达 E 节点的距离（4+1=5）要长于由 H 节点经 F 节点到达 E 节点的距离（2+2=4），所以经过后面的计算发现，在前面把 G 节点标识为永久节点是错误的，这时要把 F 节点标识为工作节点（箭头移到 F），撤销 G 节点永久工作节点的资格，如图 12-17 所示。

⑤ 再检查与 F 节点相连接的相邻节点，除了原来已标识为永久性节点的 E 外，其余就是 C 和 H 这两个临时节点了。重新计算它们到节点 A 间的距离，得到的值分别为 9 和 8。这里还要注意一个现象，就是对于 C 节点，本来属于临时节点，需要重新计算距离值，可是经过 F 节点到 A 节点的距离与原来计算所得的经过 B 节点到达 A 节点的距离是一样的，所以距离值不需要改变。此时把距离较短的 H 节点标识为工作节点（箭头移到 H）和永久性节点，如图 12-18 所示。

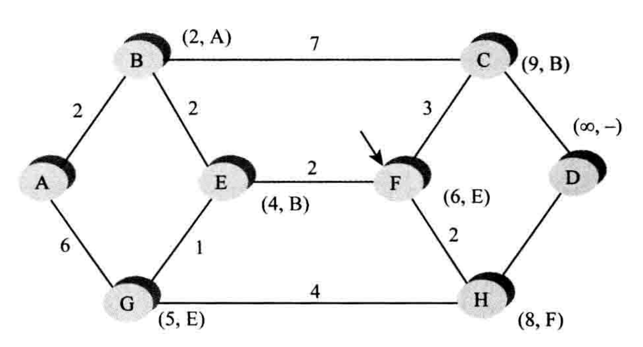


图 12-17　以 F 节点为工作节点标记其他节点与 A 节点之间的距离

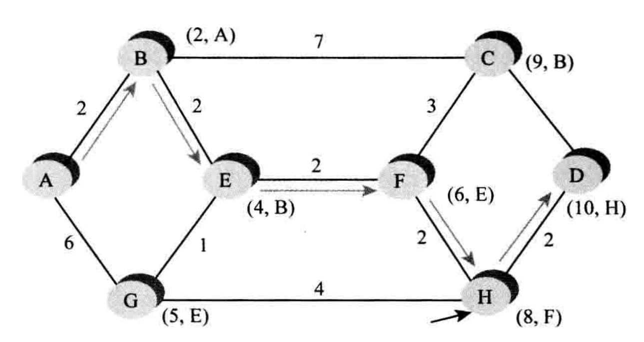


图 12-18　以 H 节点为工作节点标记其他节点与 A 节点之间的距离

此时，因为 H 节点是直接与目的节点 D 相连的，所以无需再进行选举了，直接标识 D 节点的距离为(10，H)。即从源节点 A 到目标节点 D 的最短距离就为 10，即 2+2+2+2+2，如图 12-18 所示的连线：A→B→E→F→H→D。这样，就找出了源节点到目的节点的最短距离了。

从以上可以看出，Dijkstra 算法虽然能得出最短路径，但由于它遍历计算的节点很多，所以效率低。另外，有些节点还不能一次标识正确，因为还要考虑后续节点到达源节点的距离，如以上示例中 G 节点和 F 节点的工作节点标识，最初的标识就是错误的，因为它没有考虑后续节点到源节点的距离。

2. OSPF 区域间路由计算

OSPF 路由器的 ABR 连接多了 OSPF 区域，所以它保存了多个区域的 LSDB。但是在 ABR，与所连区域内部路由器以及其他区域内路由器的通信都不是像区域内部那样是以具体的明细路由进行的，而是采用聚合路由进行的。

在 ABR 上会以 Type3 LSA（即网络聚合 LSA）的方式向所连区域内以及其他区域通告所连区域的网络聚合路由，其他区域的路由也是以 Type3 LSA 方式向所连区域内通告的。所以，区域内路由器与 ABR 以及 ABR 与其他区域的通信都是以网络聚合路由进行的。但是要注意的是，两个非骨干区域之间是不能直接进行 LSA 通告的，而是必须借助骨干区域进行转发，同样，两个非骨干区域之间是不能直接进行路由通信的，必须借助骨干区域的路由转发。所以在区域间的路由路径中一定会包括到达骨干区域对应路由器所连接网段的路由。

OSPF 区域间的路由将按照以下过程进行。

① 在源区域内部的路由器按照到达最近 ABR 的开销最小的网络聚合路由进行通信。

② 骨干区域按照到达连接到包含目的主机IP地址所在区域最近ABR的开销最小的网络聚合路由进行通信。

③ 包含目的主机 IP 地址的 ABR 按照到达目的主机的开销最小网络聚合路由进行通信。

在图 12-19 中，由 Area1 中 IP 地址为 192.168.1.10/26 的 HostA 发往位于 Area2 中的 IP 地址为 172.16.2.10/24 的 HostB 的数据报文最先从 Area1 中的内部路由器以一个网络聚合地址（这个可以由管理员在 R1 上配置，假设为 192.168.1.0/24）到达 R1（ABR/骨干路由器），然后数据报文再通过骨干区域 Area0 中的路由器转发到 R2。最后，数据报文通过聚合路由（这个也可以由管理员在 R2 上配置，假设为 172.16.0.0/16）转发，然后通过 Area2 中的内部路由器到达目的主机。

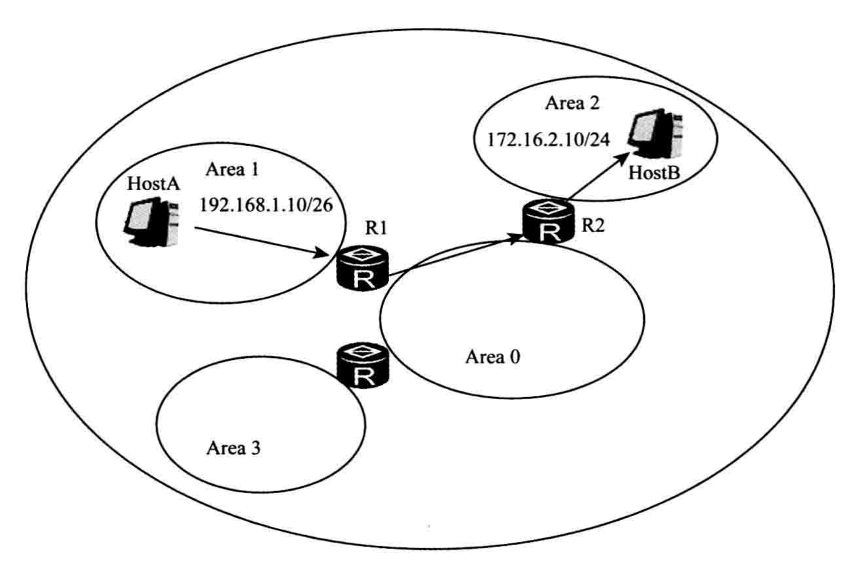


图 12-19 OSPF 区间路由示例

3. OSPF 路由维护

当链路状态发生变化时，OSPF 通过泛洪过程广播给网络上的其他路由器。OSPF 路由器接收到包含有新信息的链路状态更新报文，将更新自己的链路状态数据库，然后用 SPF 算法重新计算路由表。在重新计算过程中，路由器继续使用旧路由表，直到 SPF 完成新的路由表计算。新的链路状态信息将发送给其他路由器。值得注意的是，即使链路状态没有发生改变，OSPF 路由信息也会自动更新，缺省时间为 30 min。

12.3.4 理解 OSPF 进程

在动态路由协议中有一个路由进程的概念，一个路由器可以创建多个路由进程，那多个进程有什么用，而不同进程之间又有什么区别和联系呢？相信许多读者朋友并不真正了解。

1. 不同进程之间不相互交换路由信息，缺省是不通的

其实可以简单地把**同一路由器上**多个不同 OSPF 进程理解为多个不同的动态路由协

议的进程。我们知道，不同路由协议下的路由信息是不能直接进行交换的，最终也造成通过不同路由协议学习到的动态路由都是不通的。OSPF 上的不同进程也是如此，不同进程各自有不同的 LSDB（链路状态数据库），彼此之间是不交换路由信息的，当然彼此之间的网络也就不会直接相通了。这就是**相当于把一个物理网络划分成多个虚拟网络**。但是不同 OSPF 进程的路由是可以引入的，上章介绍的 RIP 路由中也是如此。

假设有以下这样的一个 OSPF 网络，R1、R2 和 R3 均会运行 OSPF 协议，但 R2 上配置了 10 和 20 两个进程，如图 12-20 所示。这时，如果没有配置本章后面所要讲的两个 OSPF 进程相互进行路由引入的话，R1 上连接的 192.168.1.0/24 网络是不能与 R3 上连接的 192.168.4.0/24 网络相通的，因为 R2 路由器的 S1 接口所学习到的 R1 路由器上的 192.168.1.0/24 网络路由是不会向 R3 路由器通告的，同样 R2 路由器的 S0 接口所学习到的 R3 路由器上的 192.168.4.0/24 网络路由是不会向 R1 路由器通告的。但是在 R2 上连接的两个网络还是可以直接通信的，因为它们在 R2 路由器上是直连路由，优先级最高，不需要 OSPF 协议的支持。

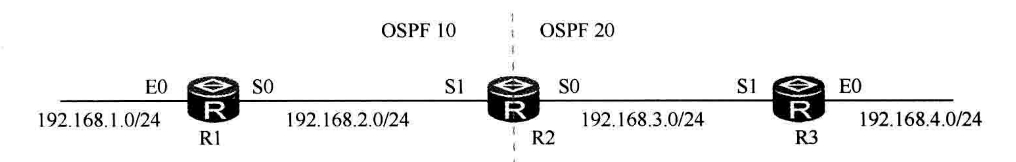


图 12-20 OSPF 进程说明示例

如果在 R2 路由器上将位于 OSPF 进程 10 的 S1 接口学习到的 OSPF 路由和直连路由引入到 OSPF 进程 20，则 R3 路由器将学习到路由 192.168.1.0/24 和 192.168.2.0/24 网络。同理，如果在 R2 路由器上将位于 OSPF 进程 20 的 S0 接口学习到的 OSPF 路由和直连路由引入到 OSPF 进程 10，则 R1 路由器将学习到路由 192.168.3.0/24 和 192.168.4.0/24 网络。

2. 路由进程仅对本地路由器有意义，相连路由器的进程可以不同

关于 OSPF 进程，我们要理解的另一个重点就是，不同的 OSPF 进程仅对本地路由器有意义，也就是它仅将本地路由器划分成多个虚拟网络。把各路由器接口划分到不同的路由进程后，对应接口只与相连路由器接口所在的 OSPF 进程中的各路由接口交换路由信息，但一定要注意的是，**相连的两个路由器接口的路由进程号可以不一样，当然也可以一样，因为进程号仅对本地路由器有意义**。如图 12-19 所示，R1 路由器的 S0 接口的 OSPF 进程号可以与 R2 路由器的 S1 接口的 OSPF 进程号一样，即都为 10，也可以不是 10，如 20、30 等都可以。同理，R3 路由器的 S1 接口 OSPF 进程号可以与 R2 路由器的 S0 接口的 OSPF 进程号一样，即都为 20，也可以不一样。

3. 同一个网络可以配置在多个 OSPF 进程中

在 OSPF 协议中，同一个直连网络可以发布在多个不同的路由进程中，也就是**一个路由器接口所连接的网络可以在多个不同的 OSPF 进程中发布**。这可能也是许多读者朋友所不了解的。这样做的目的主要是出于路由备份的考虑，使得在某一个进程下的网络不通时，对应的路由器接口所连接的网络仍然可以通过其他进程在网络中进行通信。如图 12-20 所示，R2 路由器 S0 接口可以同时发布在 10 和 20 的进程中，这样当 R3 路由器失效时，它仍然可以与 R1 路由器通信，或者通过 R1 路由器所连接的网络最终访问 R3

路由器所连接的网络。

12.4　配置 OSPF 基本功能

动态路由有一个共同的特点，那就是整个协议功能比较复杂，但是最基本的网络配置却比较简单。OSPF 路由也一样，通过简单的 OSPF 基本功能配置就可以组建起最基本的 OSPF 网络。但在配置 OSPF 的基本功能之前，需配置接口的网络层地址，使各相邻节点网络层可达。

OSPF 基本功能的配置任务和流程如下（仅前面三项必须配置，第 4 项和第 5 项配置任务没有先后次序），下面各节将分别具体介绍它们的配置步骤。

① 创建 OSPF 进程。

② 创建 OSPF 区域。

③ 使能 OSPF。

④（可选）创建虚连接。

⑤（可选）配置对 OSPF 更新 LSA 的泛洪限制。

说明 在接口视图下配置的 OSPF 命令不受 OSPF 是否使能的限制。在关闭 OSPF 后，原来在接口下配置的相关命令仍然存在。

12.4.1　创建 OSPF 进程

OSPF 是支持多进程的，要使用 OSPF 协议，首先就要创建一个 OSPF 协议进程。创建 OSPF 进程的同时要指定路由器的路由器 ID，因为一台路由器如果要运行 OSPF 协议必须存在路由器 ID。路由器 ID 是一个 IP 地址方式的 32 位无符号整数，是一台路由器在一个 AS 中的唯一标识。为保证 OSPF 运行的稳定性，在进行网络规划时应该确定路由器 ID 的划分并手动配置。

创建 OSPF 进程的方法很简单，仅需在系统视图下通过 **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] * 命令配置即可。配置此命令后将启动对应的 OSPF 进程，进入 OSPF 视图。命令中的参数说明如下。

① *process-id*：可多选参数，指定要启动的 OSPF 进程的编号，取值范围是 1～65 535 的整数，缺省值为 1。OSPF 路由器支持多进程，可以根据业务类型划分不同的进程。**但进程号是本地概念，不影响与其他路由器之间的报文交换**。因此不同的路由器之间，即使进程号不同也可以进行报文交换。

② **router-id** *router-id*：可多选参数，指定本地路由器的路由器 ID，为点分十进制格式，即 IP 地址形式，但又不起 IP 地址的作用。也可以单独用 **router id** *router-id* 系统视图命令创建路由器的路由器 ID。

说明 缺省情况下，在没有手动配置路由器 ID 情况下，系统会优先从已配置的 Loopback 接口 IP 地址中选择最大的 IP 地址作为设备的路由器 ID，如果没有配置 Loopback 接口，

则在其他物理接口 IP 地址中选取最大的 IP 地址作为设备的路由器 ID。手动配置路由器 ID 时，必须保证同一 AS 中任意两台路由器的路由器 ID 都不相同。通常的做法是将路由器 ID 配置为与该设备某个接口的 IP 地址一致。但要注意的是，**在每台 OSPF 路由器中要为每个 OSPF 进程配置一个全网唯一的路由器 ID（但同一路由器的不同进程中的路由器 ID 可以相同）**，否则会导致邻居不能正常建立、路由信息不正确的问题。

③ **instance** *vpn-instance-name*：可多选参数，指定所启动的 OSPF 进程所属的 VPN 实例的名称，1～31 个字符，区分大小写。如果不指定 VPN 实例，所启动的 OSPF 进程属于公网实例。

缺省情况下，系统不运行 OSPF 协议，即不运行 OSPF 进程，可用 **undo ospf** *process-id* [**flush-waiting-timer** *time*]命令关闭指定的 OSPF 进程，并可通过可选参数 **flush-waiting-timer** *time* 设定让其他端设备删除原来保留的该设备上的 LSA 的时间，取值范围为 1～40 的整数秒。

说明　在关闭 OSPF 进程时选择了 **flush-waiting-timer** *time* 可选参数时，设备会在设定的时间内再次产生自己的 LSA，并将其 age 字段置为 3 600（让此 LSA 立即老化）。其他设备收到 age 字段为 3 600 的 LSA 后，会立刻删除与本设备相关的 LSA。如果没有选择此可选参数，其他设备会一直保留这个 OSPF 进程中早先产生的已无效的关于本设备的 LSA，占用了系统内存，只有这些 LSA 超时（即 LSA 中的 age 字段达到 3 600 s）才会被删除。

【示例】在名为 huawei 的 VPN 实例中启动 OSPF 100 进程，进入 OSPF 视图。

```
<Huawei> system-view
[Huawei] ospf 100 router-id 10.10.10.1 vpn-instance huawei
```

12.4.2　创建 OSPF 区域

随着网络规模日益扩大，设备数量越来越多，导致 LSDB 非常庞大，设备负担很重。OSPF 协议通过将自治系统划分成不同的区域（Area）来解决上述问题。区域是从逻辑上将设备划分为不同的组，每个组用区域号（Area ID）来标识。OSPF 协议将自治系统划分成不同的区域后，同一区域内的多台设备的功能（如定时器、过滤、聚合等）就可以以区域为单位进行统一规划和配置，从而减少 LSDB 的规模，提高网络性能。但要注意：OSPF 区域的边界是设备，而不是链路，即互连设备的整个链路（包括两端的接口）只能属于一个区域，每个运行 OSPF 的接口必须指明属于哪一个区域。

OSPF 区域的创建是在对应的 OSPF 视图下进行的，创建的方法很简单，就是在对应的 OSPF 视图下使用 **area** *area-id* 命令配置。参数 *area-id* 用来指定区域的标识，**可以采用十进制整数或 IPv4 地址形式输入，但显示时使用 IPv4 地址形式**。采取整数形式时，取值范围为 0～4 294 967 295。其中 0 固定为骨干区域的 ID，**而且在一个多区域的 OSPF 网络中必须至少有一个区域 ID 为 0 的骨干区域（单区域 OSPF 网络中的区域 ID 可随意）。**骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。

缺省情况下，系统未创建 OSPF 区域，可用 **undo area** *area-id* 命令删除指定区域。

【示例】在 OSPF 100 进程下创建骨干区域 0，进入区域视图。

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 0
[Huawei-ospf-100-area-0.0.0.0]
```

12.4.3 使能 OSPF

创建 OSPF 进程后，还需要配置区域所包含的网段，也就是第 11 章介绍 RIP 路由时用 **network** 命令进行的“网络宣告”。该处的网段是指运行 OSPF 协议接口的 IP 地址所在的网段，一个网段只能属于一个区域，但这里的网络宣告与 RIP 不一样，**可以是子网和超网宣告**，而不一定需要采用自然网段进行宣告。

OSPF 路由器会对接收到的 Hello 报文做网络掩码检查，当接收到的 Hello 报文中携带的网络掩码和本设备上宣告的网络掩码不一致时，则丢弃这个 Hello 报文，即不能建立邻居关系。

OSPF 的使能既可在具体区域下一次性对一个或多个接口进行配置，也可在具体的 OSPF 接口下对一个接口进行配置。如果用两种配置方式同时配置，则对应 OSPF 接口下的配置优先级高于区域中为该接口的配置。

1. 在 OSPF 区域视图下配置

在 OSPF 区域下是通过 **network** *ip-address wildcard-mask* 命令对指定网段范围的所有 OSFP 接口一次性使能 OSPF，并指定所属的 OSPF 区域。命令中的参数说明如下。

① *ip-address*：指定要使能 OSPF 的网段 IP 地址。**接口的 IP 地址掩码长度必须≥本命令宣告网段的掩码长度。**

② *wildcard-mask*：IP 地址的反码，相当于将 IP 地址的子网掩码反转（0 变 1，1 变 0）。它是用来与参数一起确定要使能 OSPF 的网段范围的，其中，“1”表示忽略 IP 地址中对应的位，“0”表示必须匹配的位，这样就可以在一个区域内配置一个或多个接口，对应接口的主 IP 地址必须在本命令指定的网段范围之内。

说明 **本命令可多次配置，但以最后一次配置为准。**

对于 Loopback 接口，缺省情况下 OSPF 是以 32 位主机路由的方式对外发布其 IP 地址，与接口上配置的掩码长度无关。但是如果要发布 Loopback 接口的网段路由，需要在接口下执行 **ospf network-type** { **broadcast** |**nbma** } 命令配置网络类型为广播或者 NBMA。

在同一个实例的不同进程之间，或者同一个进程的不同区域之间，不能同时配置具有包含关系的两个网段。假设一个 ABR 有两个接口同在 Area1 区域，分别连接的是 192.168.1.0/24 和 192.168.3.0/24 网段，而另一个接口属于 Area0 区域，连接的网段为 192.168.4.0/24，这时在两个区域中宣告网段时均**不能采用 192.168.0.0/16**，因为这样两个区域中宣告的网段是重叠的，属于包含关系。

如果按照本节后面介绍的，在接口下通过 **ospf enable** [*process-id*] area *area-id* 命令在具体接口上使能 OSPF，则优先级高于本命令的全局使能配置。

缺省情况下，接口不属于任何区域，可用 **undo network** *address wildcard-mask* 命令从该区域中删除运行 OSPF 协议的对应接口。

【示例 1】指定接口主 IP 地址位于网段 192.168.1.0/24 的接口使能 OSPF，并加入 Area2。

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 2
[Huawei-ospf-100-area-0.0.0.2] network 192.168.1.0 0.0.0.255
```

2. 在接口视图下配置

在接口视图下使用 **ospf enable** [*process-id*] **area** *area-id* 命令使能对应接口的 OSPF 功能，指定所启动的 OSPF 进程和所加入的 OSPF 区域。

注意：在创建 OSPF 进程和配置本命令时要注意以下几个方面。

① 如果先执行本命令配置接口使能 OSPF，然后再创建对应的 OSPF 进程，虽然也可进行，**但不会自动创建对应的 OSPF 进程**。且在创建进程的时候，进程所属的 VPN 必须和本命令的接口保持一致。

② 如果先创建进程，然后执行本命令配置接口使能 OSPF，则需要检查该接口使能的进程与已经存在的进程 VPN 是否一致，如果不一致，是不允许配置的。

③ 如果没有创建进程，属于不同 VPN 实例的接口不能被使能到相同的 OSPF 进程。

缺省情况下，接口没有使能 OSPF，可用 **undo ospf enable** [*process-id*] **area** *area-id* 命令在接口上去使能 OSPF。

【示例 2】使能接口 GE1/0/0 的 OSPF 功能，并把它加入到 OSPF 1 进程的骨干区域 0 中。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf enable 1 area 0
```

12.4.4 创建虚连接

因为 OSPF 规定，在划分 OSPF 区域之后，非骨干区域之间的 OSPF 路由更新是通过骨干区域交换完成的，所以要求所有非骨干区域必须与骨干区域保持连通，并且骨干区域之间也要保持连通。但有时实际网络环境达不到这个要求，如有些区域不能与骨干区域进行直接连接，而有时骨干区域又是分离的，这时就需要通过配置 OSPF“虚连接”来解决。

虚连接支持验证，以防非法建立虚连接。具体的配置方法是在中间穿越虚连接的传输区域两端分别连接骨干区域和普通区域或者分离的骨干区域的 ABR 对应区域视图下通过 **vlink-peer** *router-id* [**smart-discover** | **hello** *hello-interval* | **retransmit** *retransmit-interval* | **trans-delay** *trans-delay-interval* |**dead** *dead-interval* | [**simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text*| [**cipher**] *cipher-text* }] | **authentication-null** | **keychain** *keychain-name*]] * 命令进行配置。命令中的参数和选项说明如下。

① *router-id*：指定建立虚连接的**对端设备**的路由器 ID。

② **smart-discover**：可多选项，设置主动发送 Hello 报文。

③ **hello** *hello-interval*：可多选参数，指定接口发送 Hello 报文的时间间隔，取值范

围为 1～65 535 的整数秒，缺省值为 10 s。但该值必须与建立虚连接路由器上的 *hello-interval* 值相等。

④ **retransmit** *retransmit-interval*：可多选参数，指定接口在发送 LSU 报文后，多长时间后没有收到 LSAck 应答报即重传原来发送的 LSA 报文，取值范围为 1～3 600 的整数秒，缺省值为 5 s。

⑤ **trans-delay** *trans-delay-interval*：可多选参数，指定接口延迟发送 LSA（为了避免频繁发送 LSA，而造成设备 CPU 负担过重）的时间间隔，取值范围为 1～3 600 的整数秒，缺省值为 1 s。

⑥ **dead** *dead-interval*：可多选参数，指定在多长时间没收到对方发来的 Hello 报文后即宣告对方路由器失效，取值范围为 1～235 926 000 的整数秒，缺省值为 40 s。**该值必须与对端设备的该参数值相等，并至少为 *hello-interval* 参数值的 4 倍。**

⑦ **simple**：多选一可选项，设置采用简单验证模式。

⑧ **plain** *plain-text*：二选一可选参数，指定采用明文密码类型。此时只能键入明文密码，在查看配置文件时也是以明文方式显示密码的。同时指定明文密码，**simple** 模式下的取值范围为 1～8 个字符，不支持空格；**md5**、**hmac-md5**、**hmac-sha256** 模式下的取值范围为 1～255 个字符，不支持空格。

⑨ **[cipher]** *cipher-text*：二选一可选参数，指定采用密文密码类型。可以键入明文或密文密码，但在查看配置文件时均以密文方式显示密码。**simple** 验证模式缺省是 **cipher** 密码类型。同时指定密文密码，**simple** 模式下的取值范围为 1～8 个字符明文密码，或者 32 个字符密文密码，不支持空格；**md5**、**hmac-md5**、**hmac-sha256** 模式下的取值范围为 1～255 个字符对应明文，20～392 个字符密文密码，不支持空格。

⑩ **md5**：多选一选项，设置采用 MD5 验证模式。缺省情况下，**md5** 验证模式缺省是 **cipher** 密码类型。

⑪ **hmac-md5**：多选一可选项，设置采用 HMAC-MD5 验证模式。缺省情况下，**hmac-md5** 验证模式缺省是 **cipher** 密码类型。

⑫ **hmac-sha256**：多选一可选项，设置采用 HMAC-SHA256 验证模式。缺省情况下，**hmac-sha256** 验证模式缺省是 **cipher** 密码类型。

⑬ *key-id*：可选参数，指定接口密文验证的验证字标识符，取值范围为 1～255 的整数，但必须与对端的验证字标识符一致。

⑭ **authentication-null**：多选一可选项，设置采用无验证模式。

⑮ **keychain** *keychain-name*：多选一可选项，设置采用 Keychain 验证模式，并指定所使用的 Keychain 的名称，长度范围为 1～47 个字符，不区分大小写。采用此验证模式前，需要首先通过 **keychain** *keychain-name* 命令创建一个 keychain，并分别通过 **key-id** *key-id*、**key-string** { [**plain**] *plain-text* | [**cipher**] *cipher-text* }和 **algorithm** { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }命令配置该 keychain 采用的 key-id、密码及其验证算法，否则会造成 OSPF 验证始终为失败状态。

缺省情况下，OSPF 不配置虚连接，可用 **undo vlink-peer** *router-id* [**dead** | **hello** | **retransmit** | **smart-discover** | **trans-delay** | [**simple** | **md5** | **hmac-md5** | **hmac-sha256** | **authentication-null** | **keychain**]]*命令删除指定虚连接或恢复指定虚连接的参数为缺

省值。

【经验之谈】别看这条命令参数选项非常多，但绝大多数参数和选项是可选的，如在虚连接中可选配置的多种不同的验证方式以及可选配置的 Hello 报文和 LSA 报文发送和接收定时器参数，但一般情况下是不需要配置验证的，也不需要重新调整这些定时器参数的，所以只需要指定对端设备的 Router ID，配置还是相当简单的。

【示例】在 Area2 区域连接骨干区域和另一个普通区域的两端 ABR 上创建虚连接，对端路由器 ID 为 1.1.1.1。

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 2
[Huawei-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

12.4.5　配置对 OSPF 更新 LSA 的泛洪限制

当邻居数量或者需要泛洪的 LSA 报文数量较多时，邻居路由器会在短时间内收到大量的 LSU 更新报文。如果邻居路由器不能及时处理这些突发的大量报文，则有可能因为忙于处理更新报文而丢弃了维护邻居关系的 Hello 报文，造成邻居断开。而这样在重建邻居时，需要交互的报文数量将会更大，由此导致报文数量过大的情况进一步恶化。此时，可通过对 OSPF 更新 LSA 的泛洪进行限制，从而有效避免以上情况的发生，起到了维护邻居关系的作用。

对 OSPF 更新 LSA 的泛洪限制是在对应的 OSPF 进程下通过 **flooding-control** [**number** *transmit-number* | **timer-interval** *transmit-interval*] * 命令进行配置的，通过本命令可设置本地设备每次泛洪更新 LSA 的数量和泛洪更新 LSA 的时间间隔。**配置本命令后，对 OSPF 更新 LSA 泛洪的限制功能将立刻生效**。命令中的参数说明如下。

① **number** *transmit-number*：可多选参数，设置每次泛洪更新 LSA 的数量，取值范围为 1～1 000 的整数，缺省值是 50。如果发现频繁有邻居路由器断开的日志提示时，可适当减小本参数值。

② **timer-interval** *transmit-interval*：可多选参数，设置每次泛洪更新 LSA 的时间间隔，取值范围为 30～100 000 ms，缺省值是 30。如果发现频繁有邻居路由器断开的日志提示时，可适当加大本参数值。

【示例】设置每次泛洪更新 LSA 的数量为 100。

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] flooding-control number 100
```

12.4.6　OSPF 基本功能管理

已经完成 OSPF 基本功能的配置后，可通过以下视图命令查看相关配置，验证配置结果。

① **display ospf** [*process-id*] **peer**：查看指定进程或所有进程下的 OSPF 邻居信息。

② **display ospf** [*process-id*] **interface**：查看指定进程或所有进程下的 OSPF 接口信息。

③ **display ospf** [*process-id*] **routing**：查看指定进程或所有进程下的 OSPF 路由表信息。

④ **display ospf** [*process-id*] **lsdb**：查看指定进程或所有进程下的 OSPF LSDB 信息。

12.4.7 OSPF 基本功能配置示例

本示例的基本拓扑结构如图 12-21 所示，所有的路由器都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 RouterA 和 RouterB 作为 ABR 来转发区域之间的路由。配置完成后，每台路由器都应学到 AS 内到所有网段的路由。

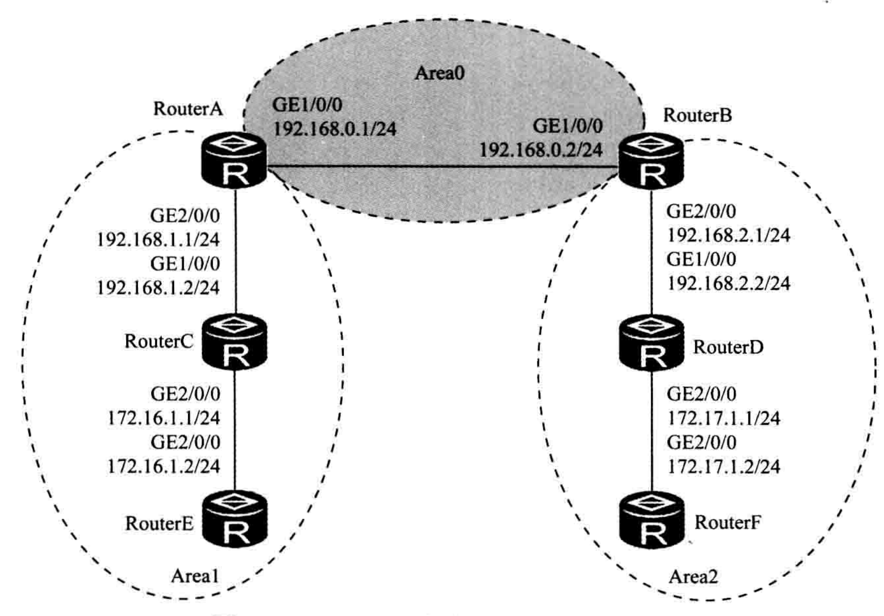


图 12-21 OSPF 基本功能配置示例拓扑结构

1. 基本配置思路分析

OSPF 基本功能的配置很简单，主要就是按照 12.4.1 小节介绍的方法创建 OSPF 进程，按照 12.4.2 小节介绍的方法创建所需的区域，按照 12.4.3 小节介绍的方法在路由器或者对应接口上使能 OSPF。但在进行这些配置之前还需要配置好各路由器接口 IP 地址。

本示例采用在区域视图下使能 OSPF 的方式进行配置，不在具体接口上进行单独使能。

2. 具体配置步骤

① 配置各路由器接口 IP 地址。下面仅以 RouterA 上的接口配置为例进行介绍，RouterB、RouterC、RouterD、RouterE 和 RouterF 的配置方法一样，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.0.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

② 配置 OSPF 基本功能。因为本示例中都是单进程，所以在创建 OSPF 进程时，进程号可以不写，都采用缺省的 1 号进程。

RouterA 上的配置：RouterA 属于 ABR，所以要分别创建所连接的两个区域，并在每个区域中宣告区域中接口所连接的网段。

```
[RouterA] ospf router id 1.1.1.1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit
```

【经验之谈】在配置 OSPF 基本功能时，最关键的一点就是各 OSPF 接口的网段通告。与第 11 章介绍的 RIP 接口网段通告类似，可以通过一条 **network** 命令对多个连接在同一网段下的各子接口进行一次性通告。但 OSPF 中的 **network** 命令与 RIP 中的 **network** 命令存在较大不同。RIP 中所通告的路由只能是自然网段的路由，通告网段路由是不带子网掩码的，因为是直接采用对应 IP 地址所在的自然网段的子网掩码；而 OSPF 中所通告的路由可以是对应的自然网段，甚至超网路由，具体由在通告网段路由时所**必须同时指定**的 IP 地址及反码（也就是通常所说的“通配符掩码”）一起来指定。

另外，在 OSPF 网段通告时要特别注意的是，**在不同区域、不同进程中所通告的网段路由不能有包含、交叉关系，当然更不能是完全重叠关系（这种情况主要发生在连接多个区域的 ABR 上）**。如本示例中的 RouterA 上的 GE1/0/0 接口所连接的网段是 192.168.0.0/24，GE2/0/0 接口连接的网段是 192.168.1.0/24，如果它们是在同一区域中，则完全可以用 192.168.0.0/16 的路由进行通告，但因为现在它们是在不同区域中，所以两个区域中都不能这样宣告，只能分别宣告，以免重叠。同时，如果两个接口位于不同 OSPF 进程，也一样不能宣告成 192.168.0.0/16 路由的，因为这样两个进程所宣告的网段就是重叠的了。本示例中的 RouterB 也一样。

RouterB 上的配置：与 RouterA 一样属于 ABR，配置方法也一样。

```
[RouterB] ospf router id 2.2.2.2
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] area 2
[RouterB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.2] quit
```

RouterC 上的配置：它属于 Area1 区域的内部路由器，所以仅需要创建 Area1 区域，并对其中的接口连接的网段进行宣告。

```
[RouterC] ospf router id 3.3.3.3
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] quit
```

RouterD 上的配置：与 RouterC 一样属于区域内部路由器，配置方法也一样。

```
[RouterD] ospf router id 4.4.4.4
[RouterD-ospf-1] area 2
[RouterD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.2] quit
```

RouterE 上的配置：与 RouterC 一样属于区域内部路由器，配置方法也一样。

```
[RouterE] ospf router id 5.5.5.5
[RouterE-ospf-1] area 1
[RouterE-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.1] quit
```

RouterF 上的配置：与 RouterC 一样属于区域内部路由器，配置方法也一样。

```
[RouterF] ospf router id 6.6.6.6
[RouterF-ospf-1] area 2
[RouterF-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[RouterF-ospf-1-area-0.0.0.2] quit
```

通过以上简单的配置就完成了整个网络的 OSPF 基本路由配置。下面可以在各路由器上通过 **display ospf peer** 视图命令查看各自的 OSPF 邻居。下面是 RouterA 上的输出示例，从中可以看出，它与 RouterB 和 RouterC 建立了完全（Full）的邻接关系（**参见粗体字部分的输出信息**）。

```
[RouterA] display ospf peer
         OSPF Process 1 with Router ID 1.1.1.1
                 Neighbors
 Area0.0.0.0 interface 192.168.0.1(GigabitEthernet1/0/0)'s neighbors
Router ID: 2.2.2.2          Address: 192.168.0.2
   State: Full   Mode:Nbr is   Master   Priority: 1
   DR: 192.168.0.2  BDR: 192.168.0.1     MTU: 0
   Dead timer due in 36   sec
   Retrans timer interval: 5
   Neighbor is up for 00:15:04
   Authentication Sequence: [ 0 ]
                 Neighbors
 Area0.0.0.1 interface 192.168.1.1(GigabitEthernet2/0/0)'s neighbors
Router ID: 3.3.3.3          Address: 192.168.1.2
   State: Full   Mode:Nbr is   Master   Priority: 1
   DR: 192.168.1.2  BDR: 192.168.1.1     MTU: 0
   Dead timer due in 39   sec
   Retrans timer interval: 5
   Neighbor is up for 00:07:32
   Authentication Sequence: [ 0 ]
```

也可以使用 **display ospf routing** 视图命令在各路由器上查看各自的 OSPF 路由信息。下面是 RouterA 的输出示例，从中可以看出它已建立了到达所有**非直连网段（直连网段的路由不会在 OSPF 路由表中出现，仅会出现的在 IP 路由表中）**的 OSPF 路由，表明以上配置是成功的。

```
[RouterA] display ospf routing
         OSPF Process 1 with Router ID 1.1.1.1
                  Routing Tables
 Routing for Network
 Destination       Cost  Type        NextHop        AdvRouter      Area
 172.16.1.0/24     2     Transit     192.168.1.2    3.3.3.3        0.0.0.1
 172.17.1.0/24     3     Inter-area  192.168.0.2    2.2.2.2        0.0.0.0
 192.168.0.0/24    1     Transit     192.168.0.1    1.1.1.1        0.0.0.0
 192.168.1.0/24    1     Transit     192.168.1.1    1.1.1.1        0.0.0.1
 192.168.2.0/24    2     Inter-area  192.168.0.2    2.2.2.2        0.0.0.0
 Total Nets: 5
 Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

还可通过 **display ospf lsdb** 视图命令查看各路由器上的 LSDB。下面是 RouterA 上的输出示例，从中可以看出，在 RouterA 上分别为所连接的 Area0 和 Area1 保存 LSDB，

其中 LinkState ID 代表链路 ID，但不同 LSA 所代表的含义不同，具体参见 12.2.6 小节说明。AdvRouter 为发布对应 LSA 的源路由器的路由器 ID。

```
[RouterA] display ospf lsdb
          OSPF Process 1 with Router ID 1.1.1.1
                  Link State Database
                          Area: 0.0.0.0
 Type      LinkState ID    AdvRouter        Age  Len   Sequence   Metric
 Router    2.2.2.2         2.2.2.2          317  48    80000003    1
 Router    1.1.1.1         1.1.1.1          316  48    80000002    1
 Network   192.168.0.2     2.2.2.2          399  32    800000F8    0
 Sum-Net   172.16.1.0      1.1.1.1          250  28    80000001    2
 Sum-Net   172.17.1.0      2.2.2.2          203  28    80000001    2
 Sum-Net   192.168.2.0     2.2.2.2          237  28    80000002    1
 Sum-Net   192.168.1.0     1.1.1.1          295  28    80000002    1
                          Area: 0.0.0.1
 Type      LinkState ID    AdvRouter        Age  Len   Sequence   Metric
 Router    5.5.5.5         5.5.5.5          214  36    80000004    1
 Router    3.3.3.3         3.3.3.3          217  60    80000008    1
 Router    1.1.1.1         1.1.1.1          289  48    80000002    1
 Network   192.168.1.1     1.1.1.1          202  28    80000002    0
 Network   172.16.1.1      3.3.3.3          670  32    80000001    0
 Sum-Net   172.17.1.0      1.1.1.1          202  28    80000001    3
 Sum-Net   192.168.2.0     1.1.1.1          242  28    80000001    2
 Sum-Net   192.168.0.0     1.1.1.1          300  28    80000001    1
```

12.4.8　OSPF 虚连接配置示例

本示例的基本拓扑结构如图 12-22 所示，Area2 没有与骨干区域直接相连。Area1 被用作传输区域（Transit Area）来连接 Area2 和 Area0。为了使 Area2 与骨干区域连通，需要在 RouterA 和 RouterB 之间配置一条虚连接（Virtual Link）。

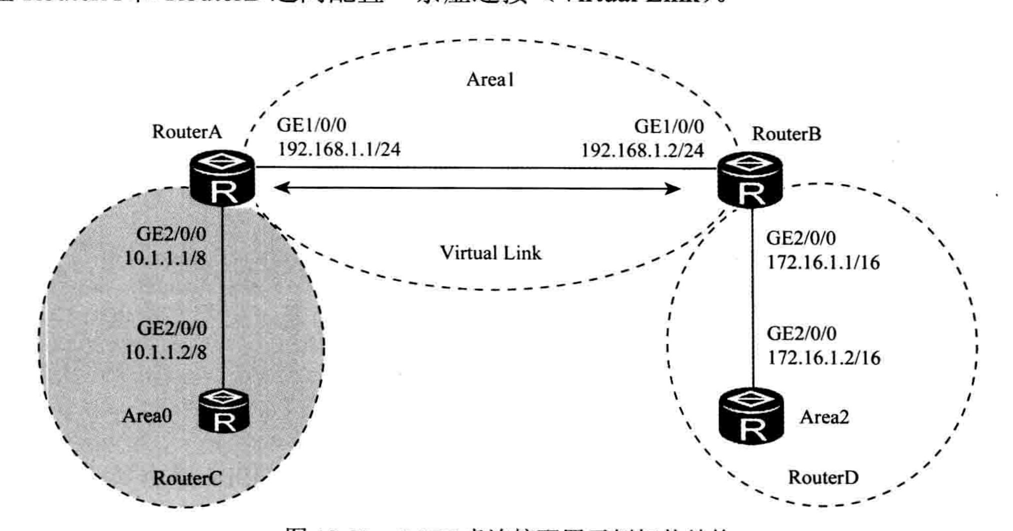


图 12-22　OSPF 虚连接配置示例拓扑结构

1．基本配置思路分析

OSPF 虚连接需要在配置 OSPF 基本功能的基础上进行配置，所以首先也需要配置各路由器的 OPSF 基本功能，使各路由器通过 OSPF 协议三层互通，然后在 RouterA 和

RouterB 上分别配置虚连接，使非骨干区域与骨干区域连通。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口 IP 地址配置为例进行介绍，RouterB、RouterC 和 RouterD 的配置方法一样，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 8
[RouterA-GigabitEthernet2/0/0] quit
```

② 配置 OSPF 基本功能。因为本示例中都是单进程，所以在创建 OSPF 进程时，进程号可以不写，都采用缺省的 1 号进程。

RouterA 上的配置：RouterA 属于 ABR，所以要分别创建所连接的两个区域，并在每个区域中宣告区域中接口所连接的网段。

```
[RouterA] ospf router-id 1.1.1.1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit
```

RouterB 上的配置：与 RouterA 一样属于 ABR，配置方法也一样。

```
[RouterB] ospf router-id 2.2.2.2
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.1] quit
[RouterB-ospf-1] area 2
[RouterB - ospf-1-area-0.0.0.2] network 172.16.0.0 0.0.255.255
[RouterB - ospf-1-area-0.0.0.2] quit
```

RouterC 上的配置：它属于骨干区域的内部路由器，所以仅需要创建 Area0 区域，并对其中的接口连接的网段进行宣告。

```
[RouterC] ospf router-id 3.3.3.3
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterC-ospf-1-area-0.0.0.0] quit
```

RouterD 上的配置：与 RouterC 一样属于区域内部路由器，配置方法也一样。

```
[RouterD] ospf router-id 4.4.4.4
[RouterD-ospf-1] area 2
[RouterD-ospf-1-area-0.0.0.2] network 172.16.0.0 0.0.255.255
[RouterD-ospf-1-area-0.0.0.2] quit
```

此时可通过 **display ospf routing** 视图命令查看 RouterA 的 OSPF 路由表。由于 Area2 没有与 Area0 直接相连，所以 RouterA 的路由表中没有 Area2 中的路由。

```
[RouterA] display ospf routing
          OSPF Process 1 with Router ID 1.1.1.1
                    Routing Tables
 Routing for Network
 Destination        Cost  Type        NextHop         AdvRouter       Area
```

```
10.0.0.0/8          1   Transit     10.1.1.1       1.1.1.1      0.0.0.0
192.168.1.0/24      1   Transit     192.168.1.1    1.1.1.1      0.0.0.1
Total Nets: 2
Intra Area: 2   Inter Area: 0   ASE: 0   NSSA: 0
```

③ 配置虚连接，需要在 RouterA 和 RouterB 上同时配置。

RouterA 上的配置如下。

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[RouterA-ospf-1-area-0.0.0.1] quit
```

RouterB 上的配置如下。

```
[RouterB] ospf
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] vlink-peer 1.1.1.1
[RouterB-ospf-1-area-0.0.0.1] quit
```

现在通过 **display ospf routing** 视图命令查看 RouterA 上的 OSPF 路由表，从中可以发现 RouterA 已通过 OSPF 协议学习到了 Area2 中的路由（**参见输出信息中的粗体部分**），证明虚连接的配置是成功的。

```
[RouterA] display ospf routing
            OSPF Process 1 with Router ID 1.1.1.1
                    Routing Tables
Routing for Network
Destination        Cost  Type        NextHop        AdvRouter     Area
172.16.0.0/16      2     Inter-area  192.168.1.2    2.2.2.2       0.0.0.2
10.0.0.0/8         1     Transit     10.1.1.1       1.1.1.1       0.0.0.0
192.168.1.0/24     1     Transit     192.168.1.1    1.1.1.1       0.0.0.1
Total Nets: 3
Intra Area: 2   Inter Area: 1   ASE: 0   NSSA: 0
```

12.5　配置 OSPF 邻居或邻接的会话参数

在 OSPF 网络中，所有链路状态信息都在邻居或邻接中传递、交换。虽然邻居或邻接的会话参数都有对应的缺省值，但在具体的网络中，根据实际网络环境，合理地配置这些参数对整网的稳定性起着重要作用。但一般情况下，不用配置本项配置任务，**即本项配置任务为可选配置**。可根据实际网络环境选择以下任务中的一项或两项进行配置。

① 配置 OSPF 报文重传限制。

② 使能在 DD 报文中填充接口的实际 MTU。在配置 OSPF 邻居或邻接关系的会话参数之前，需完成以下任务。

① 配置链路层协议。

② 配置接口的网络层地址，使各相邻节点网络层可达。

③ 配置 OSPF 的基本功能。

1. 配置 OSPF 报文重传限制

OSPF 路由器在发送完 DD、LSR 和 LSU 这三种报文后，如果没有在规定时间内收到相应的 LSAck，报文会再次重传。当达到限定报文重传次数后，本端就断开和对方的

邻接关系。为此可以调整最大的 DD、LSR 和 LSU 报文的重传次数，以避免频繁出现邻接关系断开的现象。

配置最大的 DD、LSR 和 LSU 报文的重传次数的方法很简单，仅需在对应的 OSPF 进程下使用 **retransmission-limit** [*max-number*]命令进行配置即可。可选参数 *max-number* 的取值范围是 2～255 的整数，缺省值是 30。

缺省情况下，最大重传限制数的缺省值是 30，可用 **undo retransmission-limit** 命令取消恢复为缺省的重传次数。可使用 **display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*] [**low-level-of-retrans-times-range** *min-time*] [**high-level-of-retrans-times-range** *max-time*]命令查看指定或者所有的 OSPF 重传列表。

【示例 1】在 OSPF 进程 100 下配置最大的报文重传限制数为 40。

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] retransmission-limit 40
```

2. 使能在 DD 报文中填充接口的实际 MTU

DD 报文中的 Interface MTU 字段（参见 12.2.3 小节）填写的是接口的 MTU 值，缺省为 0（代表不配置），但是在网络中存在不同厂商设备，建立虚连接时，不同的设备制造商可能会使用不同的 MTU 缺省设置。为此，有时需要取消设备缺省为 0 的 MTU 值。

取消采用缺省为 0 的 MTU 值的方法是在对应接口视图下执行 **ospf mtu-enable** 命令，使能接口发送 DD 报文时填充 MTU 值，即使用接口的实际 MTU 值填写。**配置本命令后，系统会自动重启 OSPF 进程，也会使邻居关系重新建立，所以通常不建议修改。可用 undo ospf mtu-enable** 命令恢复缺省设置。

【示例 2】指定 GE1/0/0 接口在发送 DD 报文时，填写实际的 MTU 值。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf mtu-enable
```

12.6 配置 OSPF 在不同网络类型中的属性

OSPF 支持 Broadcast、NBMA、P2P、P2MP 4 种类型的网络，具体参见 12.1.5 小节。通过配置 OSPF 接口的网络类型和调整属性可以灵活组建 OSPF 网络。

通过 12.1.5 小节表 12-2 中介绍的 OSPF 协议 4 种网络类型的特点可以看出，它们的差异主要集中在发送报文形式不同，因此，在 4 种网络类型中配置的 OSPF 协议，主要区别就是体现在协议报文的发送形式上。在不同网络类型属性的配置中，主要包括以下三项配置任务，且配置接口的网络类型是配置 P2MP 和 NBMA 网络属性的前置任务。

① 配置接口的网络类型。

② 配置 P2MP 网络属性。

③ 配置 NBMA 网络属性。

同样，在配置 OSPF 在不同网络类型中的属性之前，需完成以下任务。

① 配置接口的网络层地址，使各相邻节点网络层可达。

② 配置 OSPF 的基本功能。

12.6.1　配置接口的网络类型

配置接口的网络方法很简单，只需在对应接口视图下通过 **ospf network-type { broadcast | nbma | p2mp | p2p }**命令配置即可。命令的四个多选一选项分别代表广播网络类型、NBMA 网络类型、P2MP 网络类型和 P2P 网络类型。当用户为接口配置了新的网络类型后，原接口的网络类型将被替换。

缺省情况下，接口的网络类型是根据物理接口类型而定的，即以太网接口的网络类型为广播，串口和 POS 口（封装 PPP 协议或 HDLC 协议时）的网络类型为 P2P，ATM 和 Frame-relay（帧中继）接口的网络类型为 NBMA。可用 **undo ospf network-type** 命令恢复 OSPF 接口为缺省的网络类型。

可根据实际情况配置接口的网络类型，但也不是随意的，具体要考虑以下几个方面。

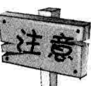
① 如果同一网段内只有两台设备运行 OSPF 协议，也可以将接口的网络类型改为 P2P。

② 如果接口的网络类型是广播，但在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为 NBMA。

③ 如果接口的网络类型是 NBMA，且网络是全连通的，即任意两台路由器都直接可达。此时，可以将接口类型改为 Broadcast，并且不必再配置邻居路由器。

④ 如果接口的网络类型是 NBMA，但网络不是全连通的，必须将接口的网络类型改为 P2MP。这样，两台不能直接可达的路由器就可以通过一台与两者都直接可达的路由器来交换路由信息。**接口的网络类型改为 P2MP 网络后，不必再配置邻居路由器。**

⑤ 如果同一网段内只有两台路由器运行 OSPF 协议，建议将接口的网络类型改为 P2P。



在配置网络类型时，要注意以下几个方面。

① P2MP 网络类型必须是由其他的网络类型强制更改的。

② AR150/160/200 系列不支持 Frame-relay 接口。

③ 一般情况下，链路两端的 OSPF 接口的网络类型必须一致，否则不可以建立起邻居关系。

④ 当链路两端的 OSPF 接口的网络类型一端是 Broadcast，另一端是 P2P 时，仍可以正常地建立起邻居关系，但互相学习不到路由信息。

⑤ 当链路两端的 OSPF 接口的网络类型一端是 P2MP，另一端是 P2P 时，仍可以正常地建立起邻居关系，但互相学习不到路由信息。为了相互学习到路由信息，此时需要在链路两端的 OSPF 接口上配置相同的 Hello 报文发送间隔和邻居失效时间。

【示例 1】将 GE1/0/0 接口设置为 NBMA 类型。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf network-type nbma
```

另外，在 **Broadcast** 网络中可以通过 **ospf dr-priority** *priority* 接口视图命令配置路由器的优先级，用于 DR 和 BDR 选举。参数 *priority* 用来指定接口在选举 DR 或 BDR 时的优先级。其值越大，优先级越高，取值范围是 0～255 的整数。**如果一台设备的接口优先**

级为 0，则它不会被选举为 DR 或 BDR。在广播或 NBMA 网络中，也可以通过配置接口的 DR 优先级来影响网络中 DR 或 BDR 的选择，具体将在 12.6.3 小节介绍。

【示例 2】设置 GE1/0/0 接口在选举 DR 时的优先级为 8。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf dr-priority 8
```

12.6.2 配置 P2MP 网络属性

缺省情况下，在 P2MP 网络上，接口 IP 地址的子网掩码长度不一致的设备不可以建立邻居关系。但可以通过配置设备间忽略对 Hello 报文中网络掩码（参见 12.2.2 小节图 12-5）的检查，就可以正常建立 OSPF 邻居关系了。另外，在 P2MP 网络中，当两台路由器之间存在多条链路时，通过对出方向的 LSA 进行过滤可以减少 LSA 在某些链路上的传送，减少不必要的重传，节省带宽资源。这两项功能的具体配置步骤如表 12-8 所示。

表 12-8　　P2MP 网络属性配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface gigabitethernet 1/0/0**	键入要配置为 P2MP 网络类型的接口，进入接口视图
3	**ospf network-type p2mp** 例如：[Huawei-GigabitEthernet1/0/0] **ospf network-type p2mp**	配置以上接口为 P2MP 网络类型。**P2MP 网络类型必须是由其他的网络类型强制更改的**，可用 **undo ospf network-type** 命令恢复 OSPF 接口为缺省的网络类型
4	**quit** 例如：[Huawei-GigabitEthernet1/0/0] **quit**	退出接口视图，返回系统视图
5	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
6	**filter-lsa-out peer** *ip-address* { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }]| **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** { *acl-number* | *acl-name* }] } * } 例如：[Huawei-ospf-10] **filter-lsa-out peer** 10.1.1.1 **all**	配置在 P2MP 网络中对发送的 LSA 进行过滤。命令中的参数和选项说明如下 ● *ip-address*：指定要过滤发送 LSA 的 P2MP 邻居的 IP 地址，不向这个邻居发送 LSA ● **all**：二选一可选项，指定对除 Grace-LSA 之外的所有 LSA 进行过滤 ● **summary**：可多选选项，指定对 Type3 LSA 进行过滤 ● **ase**：可多选选项，指定对 Type5 LSA 进行过滤 ● **nssa**：可多选选项，指定对 Type7 LSA 进行过滤 ● **acl** { *acl-number* | *acl-name* }：可选参数，指定用于对要发送的 Type3 LSA 或者 Type5 LSA 或者 Type7 LSA 进行过滤的 ACL 表号（取值范围为 2 000～2 999）或者 ACL 名称（1～32 个字符，但**开头第一个字母必须以英文字母形式，区分大小写**），用 source 参数过滤发送的 LSA 中的 IP 报头源 IP 地址范围。对于使用命名型 ACL 中的规则进行过滤时，只有 source 参数指定的源地址范围和 time-range 参数指定的时间段对配置规则过滤规则有效

（续表）

步骤	命令	说明
6	**filter-lsa-out peer** *ip-address* { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }]| **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** { *acl-number* | *acl-name* }] } * } 例如：[Huawei-ospf-10] **filter-lsa-out peer** 10.1.1.1 **all**	【说明】Grace LSA 用于在开始和退出 GR 时向邻居通告 GR（Graceful Restart，平滑启动）的时间、原因、接口实例 ID 等内容，不能对 Grace LSA 进行过滤 缺省情况下，在 P2MP 网络中不对指定邻居发送的 LSA 进行过滤，可用 **undo filter-lsa-out peer** *ip-address* 命令取消在 P2MP 网络中对指定邻居发送的 LSA 进行过滤

说明　GR（Graceful Restart，平滑重启）是一种冗余容错技术，目前已经被广泛地使用在主备切换和系统升级方面，以保证关键业务的不间断转发。OSPF 通过新增 Grace-LSA 来支持 GR 功能。这种 LSA 用于在开始 GR 和退出 GR 时向邻居通告 GR 的时间、原因以及接口地址等内容。

12.6.3　配置 NBMA 网络属性

NBMA 网络属性配置主要可以包括以下三项配置任务。

1. （可选）配置 NBMA 网络类型

当确定某 OSPF 接口连接的是 NBMA 网络时，可以配置该接口的网络类型为 NBMA。但要注意的是，NBMA 网络必须是全连通的，所以网络中任意两台路由器之间都必须直接可达（无需经过其他中间路由器）。如果这个要求无法满足，则必须通过命令强制将网络的类型改变为 P2MP。

2. （可选）配置 NBMA 网络发送轮询报文的时间间隔

在 NBMA 网络上，当邻居失效后，路由器将按设置的轮询时间间隔定期地发送 Hello 报文。但因为有缺省配置，所以本项配置任务也是可选的。

3. 配置 NBMA 网络的邻居

当网络类型为 NBMA（例如 X.25 或帧中继网络）时，可以通过配置映射使整个网络达到全连通状态（即网络中任意两台设备之间都存在一条虚电路且直接可达）。这样，OSPF 就可以看作是广播网络进行 DR、BDR 选举等。但由于无法通过广播 Hello 报文的形式动态发现相邻设备，必须手动通过 **peer** 命令指定相邻设备的 IP 地址以及用于 DR 选举的优先级。

以上三项配置任务的具体配置步骤如表 12-9 所示。

表 12-9　NBMA 网络属性的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
（可选）配置 NBMA 网络类型	2	**interface** *interface-type interface-number* 例如：[Huawei] **interface gigabitethernet 1/0/0**	键入要配置为 NBMA 网络类型的接口，进入接口视图

（续表）

配置任务	步骤	命令	说明
（可选）配置NBMA网络类型	3	**ospf network-type nbma** 例如：[Huawei-GigabitEthernet1/0/0] **ospf network-type nbma**	配置以上接口为NBMA网络类型，可用**undo ospf network-type**命令恢复OSPF接口为缺省的网络类型
（可选）配置NBMA网络发送轮询Hello报文的时间间隔	4	**ospf timer poll** *interval* 例如：[Huawei-GigabitEthernet1/0/0] **ospf timer poll** 150	配置NBMA网络上发送轮询Hello报文的时间间隔，取值范围为1～3 600整数秒。轮询Hello报文的发送时间间隔值至少应为Hello报文发送时间间隔的4倍 缺省情况下，时间间隔为120 s，可用**undo ospf timer poll**命令恢复发送轮询Hello报文间隔的缺省值
	5	**quit** 例如：[Huawei-GigabitEthernet1/0/0] **quit**	退出接口视图，返回系统视图
配置NBMA网络的邻居	6	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的OSPF进程，进入OSPF视图
	7	**peer** *ip-address* [**dr-priority** *priority*] 例如：[Huawei-ospf-10] **peer** 1.1.1.1	配置NBMA网络的邻居，**需要重复使用本命令指定其他邻居**。命令中的参数说明如下 ● *ip-address*：指定邻居的接口主IP地址 ● **dr-priority** *priority*：指定相邻设备的优先级，用于DR选举，取值范围为0～255的整数，缺省值为1。但要注意，通过此命令设置对端设备的DR选举的优先级，**必须与本端设备的DR的优先级一致** 缺省情况下，没有在NBMA网络上指定相邻路由器的IP地址，也没有配置DR选举权，可用**undo peer** *ip-address*命令取消指定IP地址的设备为接口的邻居路由器

12.6.4 OSPF网络属性管理

在已经完成OSPF在NBMA网络和P2MP网络中的属性的所有配置后，可以通过以下**display**任意视图命令查看相关配置信息，验证配置结果。

① **display ospf** [*process-id*] **lsdb** [**brief**]或**display ospf** [*process-id*] **lsdb** [{ **router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** |**opaque-as** } [*link- state-id*]] [**originate-router** [*advertising-router-id*] | **self-originate**] [**age** { **min-value** *min-age-value* | **max-value** *max-age-value* } *]：查看指定的或者所有OSPF的链路状态数据库（LSDB）信息。

② **display ospf** [*process-id*] **peer** [[*interface-type interface-number*] *neighbor-id* | **brief** | **last-nbr-down**]：查看指定的或者所有OSPF邻居的信息。

③ **display ospf** [*process-id*] **nexthop**：查看指定进程或者所有进程下OSPF的下一跳信息。

④ **display ospf** [*process-id*] **routing router-id** [*router-id*]或**display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop**

nexthop-address]：查看指定的或者所有 OSPF 路由表的信息。

⑤ **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]：查看指定的或者所有 OSPF 的接口信息。

12.6.5　OSPF 的 DR 选举配置示例

本示例的拓扑结构如图 12-23 所示，在一个广播型 OSPF 网络中，配置 RouterA 的优先级为 100，这是网络上的最高优先级，被选举为 DR；RouterC 是优先级第二高的，被选为 BDR；RouterB 的优先级为 0，这意味着它将无法成为 DR 或 BDR；RouterD 没有配置优先级，取缺省值 1。

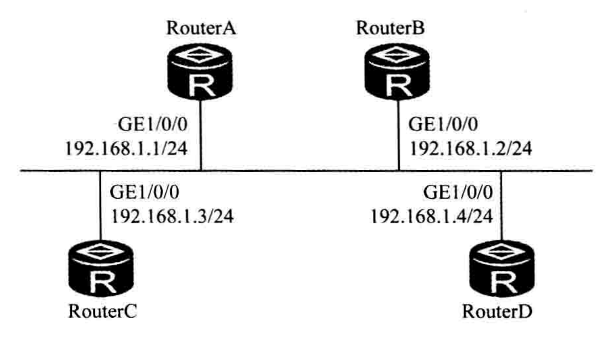


图 12-23　OSPF 的 DR 选举配置示例拓扑结构

1. 基本配置思路分析

本示例的配置很简单，首先需要在各路由器上配置 OSPF 的基本功能，使整个网络通过 OSPF 协议可达，然后分别按要求为 RouterA、RouterB 和 RouterC 配置用于 DR、BDR 选举的 DR 优先级，RouterD 直接采用缺省 DR 优先级 1，不用另外配置。要注意，**选举了 DR 和 BDR 后，区域内路由器仅与 DR、BDR 交互 LSA，DROther 之间不需要交互 LSA 的。**

2. 具体配置步骤

① 配置各接口的 IP 地址（略）。

② 分别在 4 台路由器上配置 OSPF 基本功能，均采用缺省的 OSPF 进程 1，所以在创建进程时不用写具体的进程号。然后就是宣告各区域中的接口所在网段，配置各自的路由器 ID。

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit

[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit

[RouterC] router id 3.3.3.3
```

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit

[RouterD] router id 4.4.4.4
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
```

此时可通过 **display ospf peer** 任意视图命令查看各路由器的邻居信息。下面是 RouterA 上的输出示例，因为此时它们都是直接采用缺省的优先级值 1，均为缺省状态，DR 和 BDR 角色的选举依据是路由器 ID，高的为 DR 或者 BDR，所以最终 RouterD 为 DR，RouterC 为 BDR（**参见输出信息中的粗体字部分**）。

说明 当两台路由器接口的 DR 优先级相同时，路由器 ID 高的为 DR 或者 BDR。但 DR、BDR 已经选择完毕，当一台新路由器加入后，即使它的 DR 优先级值最大，也不会立即成为该网段中的 DR，**也就是不会进行 DR 角色抢占**。

```
[RouterA] display ospf peer
          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors
 Area0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/0)'s neighbors
 Router ID: 2.2.2.2          Address: 192.168.1.2
State: Full   Mode:Nbr is   Master   Priority: 1
DR: 192.168.1.4   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 32   sec
   Retrans timer interval: 5
   Neighbor is up for 00:04:21
   Authentication Sequence: [ 0 ]
 Router ID: 3.3.3.3          Address: 192.168.1.3
State: Full   Mode:Nbr is   Master   Priority: 1
DR: 192.168.1.4   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 37   sec
   Retrans timer interval: 5
   Neighbor is up for 00:04:06
   Authentication Sequence: [ 0 ]
 Router ID: 4.4.4.4          Address: 192.168.1.4
State: Full   Mode:Nbr is   Master   Priority: 1
DR: 192.168.1.4   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 37   sec
   Retrans timer interval: 5
   Neighbor is up for 00:03:53
   Authentication Sequence: [ 0 ]
```

③ 现在重新按照示例要求配置 RouterA、RouterB 和 RouterC 接口上的 DR 优先级。

RouterA 上的配置如下。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ospf dr-priority 100
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ospf dr-priority 0
[RouterB-GigabitEthernet1/0/0] quit
```

RouterC 上的配置如下。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ospf dr-priority 2
[RouterC-GigabitEthernet1/0/0] quit
```

现在通过 **display ospf peer** 命令查看网络中的 DR/BDR 的状态。下面是 RouterD 上的输出示例，从中可以出，尽管它们的 DR 优先级进行了修改，但是 DR 和 BDR 角色仍没有变，仍是以 RouterD 为 DR，RouterC 为 BDR（**参见输出信息中的粗体字部分**），因为重新配置了 DR 优先级后要重启 OSPF 进程才能进行新的 DR 选举。

```
[RouterD] display ospf peer
          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors
 Area0.0.0.0 interface 192.168.1.4(GigabitEthernet1/0/0)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1
   State: Full   Mode:Nbr is   Slave   Priority: 100
DR: 192.168.1.4   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 31   sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:17
   Authentication Sequence: [ 0 ]
 Router ID: 2.2.2.2          Address: 192.168.1.2
   State: Full   Mode:Nbr is   Slave   Priority: 0
DR: 192.168.1.4   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 35   sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:19
   Authentication Sequence: [ 0 ]
 Router ID: 3.3.3.3          Address: 192.168.1.3
   State: Full   Mode:Nbr is   Slave   Priority: 2
DR: 192.168.1.4   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 33   sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:15
   Authentication Sequence: [ 0 ]
```

④ 在各路由器的用户视图下，同时执行 **reset ospf 1 process** 命令，以重启 OSPF 进程。此时再通过 **display ospf peer** 命令查看 OSPF 邻居状态，就会发现已是以 RouterA 为 DR，RouterC 为 BDR（**参见输出信息中的粗体字部分**）。如果邻居的状态是 Full，这说明它和邻居之间形成了邻接关系；**如果停留在 2-Way 的状态，则说明它们都不是 DR 或 BDR，两者之间不需要交换 LSA。**

```
[RouterD] display ospf peer
          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors
 Area0.0.0.0 interface 192.168.1.4(GigabitEthernet1/0/0)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1
State: Full   Mode:Nbr is   Slave   Priority: 100
DR: 192.168.1.1   BDR: 192.168.1.3   MTU: 0
   Dead timer due in 35   sec
   Retrans timer interval: 5
```

```
    Neighbor is up for 00:07:19
    Authentication Sequence: [ 0 ]
  Router ID: 2.2.2.2          Address: 192.168.1.2
 State: Full   Mode:Nbr is   Master   Priority: 0
 DR: 192.168.1.1   BDR: 192.168.1.3   MTU: 0
    Dead timer due in 35   sec
    Retrans timer interval: 5
    Neighbor is up for 00:07:19
    Authentication Sequence: [ 0 ]
  Router ID: 3.3.3.3          Address: 192.168.1.3
 State: Full   Mode:Nbr is   Slave   Priority: 2
 DR: 192.168.1.1   BDR: 192.168.1.3   MTU: 0
    Dead timer due in 37   sec
    Retrans timer interval: 5
    Neighbor is up for 00:07:17
    Authentication Sequence: [ 0 ]
```

还可通过命令查看 OSPF 接口的状态。下面分别是 RouterA 和 RouterB 上的输出示例。如果 OSPF 接口的状态是 DROther，则说明它既不是 DR，也不是 BDR。

```
[RouterA] display ospf interface
          OSPF Process 1 with Router ID 1.1.1.1
                  Interfaces
 Area: 0.0.0.0
 IP Address   Type        State    Cost  Pri   DR              BDR
 192.168.1.1 Broadcast    DR       1     100 192.168.1.1 192.168.1.3

[RouterB] display ospf interface
          OSPF Process 1 with Router ID 2.2.2.2
                  Interfaces
 Area: 0.0.0.0
 IP Address       Type        State     Cost  Pri   DR              BDR
 192.168.1.2      Broadcast   DROther   1     0 192.168.1.1 192.168.1.3
```

12.7 配置 OSPF 的 Stub/Totally Stub/NSSA/Totally NSSA 区域

通过将位于 AS 边缘的一些非骨干区域配置成 Stub 区域（包括 Totally Stub 区域）或者 NSSA 区域（包括 Totally NSSA 区域），可以缩减 LSDB 和路由表规模，减少需要传递的路由信息数量。当然，Stub 区域和 NSSA 区域都是一种可选的配置属性。

配置 Stub 区域时需要注意以下几点。

① 骨干区域（Area0）不能配置成 Stub 区域或者 NSSA 区域。

② 如果要将一个区域配置成 Stub 区域或者 NSSA 区域，则该区域中的所有路由器都要配置 Stub 区域或者 NSSA 区域属性。

③ Stub 区域内**不能有 ASBR**，即自治系统外部的路由不能在 Stub 区域内传播，**且只有一个 ABR；NSSA 区域可以有一个或者多个 ABR 和 ASBR**，允许自治系统外部的路由通过 Type7 LSA 在 NSSA 区域内传播，然后在 NSSA 区域的 ABR 上转换成 Type5 LSA 向其他 OSPF 区域传播。

④ Stub 区域和 NSSA 区域内都不能存在虚连接。

有关 Stub 区域和 NSSA 区域的特点参见本章 12.1.4 小节。

12.7.1 配置 OSPF 的 Stub/Totally Stub 区域

Stub 区域的配置很简单，主要包括以下两项配置任务：①配置当前区域为 Stub 区域；②（可选）配置发送到 Stub 区域缺省路由的开销。如果想配置为 Totally Stub 区域，则还可在 ABR 上禁止 Type3 LSA 向区域内泛洪。当区域配置为 Stub 或者 Totally Stub 区域后，为保证到达外部自治系统，或者同时包括到达其他区域（仅在配置为 Totally Stub 区域时）的路由可达，Stub 区域的 ABR 将**自动**生成一条缺省路由，并发布给 Stub 区域内的其他路由器。

以上几项配置任务的具体配置步骤如表 12-10 所示。在配置 OSPF 的 Stub 区域前，需要先配置好接口的网络层地址，使各相邻节点网络层可达，同时也要先完成 OSPF 基本功能的配置。

表 12-10　　Stub 区域配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
3	**area** *area-id* 例如：[Huawei-ospf-10] **area** 10	键入要配置为 Stub 区域的区域，进入 OSPF 区域视图
4	**stub** 例如：[Huawei-ospf-10area-0.0.0.10] **stub**	配置当前区域为 Stub 区域。**需要在区域内所有路由器上配置，包括该区域中唯一的 ABR** 【注意】所有连接到 Stub 区域的路由器必须使用 stub 命令将该区域配置成 Stub 区域属性 配置或取消 Stub 属性，可能会触发区域更新，所以只有在上一次区域更新完成后，才能进行再次配置或取消配置操作 缺省情况下，没有区域被设置为 Stub 区域。，可用 **undo stub** 命令取消对应区域为 Stub 区域
5	**stub no-summary** 例如：[Huawei-ospf-10area-0.0.0.10] **stub no-summary**	（可选）**在 Stub 区域 ABR 上**禁止向 Stub 区域内发送 Type3 LSA，**这时 Stub 区域就成为了 Totally Stub 区域** 缺省情况下，Stub 区域不禁止 Type3 LSA 向区域内泛洪，可用 **undo stub no-summary** 命令取消禁止 Type3 LSA 向区域内泛洪
6	**default-cost** *cost* 例如：[Huawei-ospf-10area-0.0.0.10] **default-cost** 10	（可选）**在 Stub 区域 ABR 上**配置发送到 Stub 区域缺省路由的开销。参数 *cost* 用来配置为发送到 Stub 区域的 Type3 缺省路由的开销，取值范围为 0～16 777 214 的整数。**当然必须在本地路由表中已存在该缺省路由** 缺省情况下，发送到 Stub 区域的 Type3 缺省路由的开销为 1，可用 **undo default-cost** 命令将 Stub 区域缺省路由的开销恢复为缺省值

12.7.2 配置 OSPF 的 NSSA/Totally NSSA 区域

NSSA 区域的配置也很简单，主要包括以下两项配置任务：①配置当前区域为 NSSA 区域；②（可选）配置发送到 NSSA 区域缺省路由的开销。如果想配置为 Totally NSSA 区域，则还可在 ABR 上禁止 Type3 LSA 向区域内泛洪。当区域配置为 NSSA 或者 Totally NSSA 区域后，**为保证到达非本区域直连的外部自治系统**，或者同时包括到达其他区域（仅当配置为 Totally NSSA 区域时）的路由可达，NSSA 区域的 ABR 将**自动**生成一条缺省路由，并发布给 NSSA 区域中的其他路由器。

以上几项配置任务的具体配置步骤如表 12-11 所示。在配置 OSPF 的 NSSA 区域之前，也需要先配置接口的网络层地址，使相邻节点之间网络层可达。同时还要配置 OSPF 的基本功能。

表 12-11　NSSA 区域配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
3	**area** *area-id* 例如：[Huawei-ospf-10] **area** 10	键入要配置为 NSSA 区域的区域，进入 OSPF 区域视图
4	**nssa** [**default-route-advertise** | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding**] * 例如：[Huawei-ospf-10area-0.0.0.10] **nssa**	配置当前区域为 NSSA 区域（**其中大多部分参数和选项均仅可在 ABR 或者 ASBR 上配置**）。命令中的参数和选项说明如下 ● **default-route-advertise**：可多选选项，**在 ASBR 上**配置产生缺省的 Type7 LSA 到 NSSA 区域。在 ABR 上会自动产生缺省的 Type7 LSA 到 NSSA 区域。但只有在 ASBR 上当路由表中存在缺省路由 0.0.0.0/0，才会产生 Type7 LSA 缺省路由 ● **flush-waiting-timer** *interval-value*：可多选参数，**在 ASBR** 上配置向 NSSA 区域内部路由器发送老化 Type5 LSA（老化时间被置为最大值——3 600 s 的 Type5 LSA）的时间间隔，取值范围为 1～40 的整数秒，用以及时清除区域内其他路由器上已经没用的 Type5 LSA（因为在 NSSA 区域中已不再支持 Type5 LSA，仅支持 Type7 LSA 了） ● **no-import-route**：可多选选项，**当 ASBR 同时还是 ABR 时**，指定不向 NSSA 区域泛洪由 **import-route** 命令引入的外部路由 ● **no-summary**：可多选选项，**在 ABR** 上禁止向 NSSA 区域内发送 Type3 LSA。**这时 NSSA 区域就成了 Totally NSSA 区域** ● **set-n-bit**：可多选选项，指定在 DD 报文中设置 N-bit 位的标志。选择本可选项后，本端路由器会在与邻居路由器同步时，在 DD 报文中设置 N-bit 位的标志，代表自己是直接连接在 NSSA 区域 ● **suppress-forwarding-address**：可多选选项，**在 ABR 上**配置将转换后生成的 Type5 LSA 的 FA（Forwarding Aaddress）设置为 0.0.0.0（抑制转发地址）

（续表）

步骤	命令	说明
4	**nssa** [**default-route-advertise** | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding**] * 例如：[Huawei-ospf-10area-0.0.0.10] **nssa**	• **translator-always**：可多选选项，**在 ABR 上**指定转换路由器。允许将 NSSA 区域中的多个 ABR 配置成转换路由器（转换路由器是用来将 Type7 LSA 转换为 Type5 LSA，然后向 OSPF 路由域中的其他区域进行通告）。当 NSSA 区域中有多个 ABR 时，系统会根据规则自动选择一个 ABR 作为转换器（通常情况下 NSSA 区域选择 Router ID 最大的设备）。如果需要指定某两个 ABR 进行负载分担，可以分别在这两台 ABR 上通过配置此可选项来指定两个转换器同时工作 • **translator-interval** *interval-value*：可多选参数，在转换路由器上配置当前转换器失效的时间，取值范围为 1～120 的整数秒，缺省值是 40 s，主要用于转换器切换，保障切换平滑进行 • **zero-address-forwarding**：可多选选项，**在 ABR 上**配置引入外部路由时将生成的 NSSA LSA 的 FA 置为 0.0.0.0 缺省情况下，OSPF 没有区域被设置成 NSSA 区域，可用 **undo nssa** [**flush-waiting-timer** *interval-value*]命令取消 NSSA 区域，恢复 OSPF 区域为普通区域
5	**default-cost** *cost* 例如：[Huawei-ospf-10area-0.0.0.10] **default-cost** 10	（可选）**在 ABR 上**配置发送到 NSSA 区域的 Type3 LSA 的缺省路由的开销。参数 *cost* 用来配置为发送到 NSSA 区域的 Type3 缺省路由的开销，取值范围为 0～16 777 214 的整数。**当然也必须本地路由表中已存在该缺省路由** 缺省情况下，发送到 NSSA 区域的 Type3 缺省路由的开销为 1，可用 **undo default-cost** 命令将 NSSA 区域缺省路由的开销恢复为缺省值

12.7.3 Stub 区域和 NSSA 区域管理

配置好 Stub 区域和 NSSA 区域后，可以通过以下 **display** 任意视图命令查看相关配置，验证配置结果。

① **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop***nexthop-address*]或 **display ospf** [*process-id*] **routing router-id** [*router-id*]：查看指定的或者所有的 OSPF 路由表的信息。

② **display ospf** [*process-id*] **abr-asbr** [*router-id*]：查看 OSPF ABR 和 ASBR 信息。

③ **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]：查看指定或所有进程下的指定或者所有 OSPF 接口信息。

12.7.4 OSPF 的 Totally Stub 区域配置示例

本示例的基本拓扑结构如图 12-24 所示，所有的路由器都运行 OSPF，整个自治系统划分为 3 个区域。其中 RouterA 和 RouterB 作为 ABR，用来转发区域之间的路由，RouterD 作为 ASBR 引入了外部静态路由（**从本示例可见 ASBR 不一定要位于区域边缘**）。现要求将 Area1 配置为 Totally Stub 区域，以最大限度地减少通告到此区域内的 LSA 数量，但又不影响与 AS 外部和其他区域间的路由的可达性。

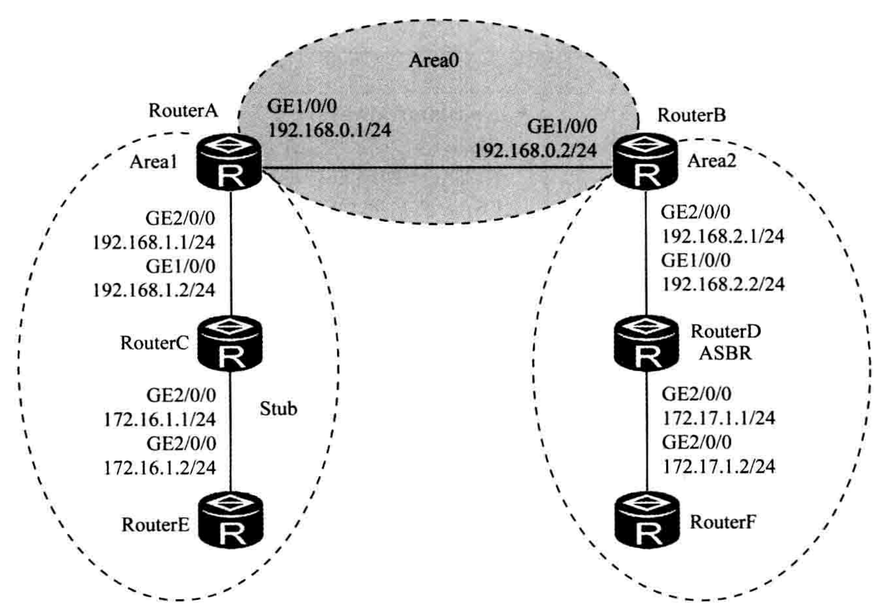


图 12-24 OSPF Stub 区域配置示例拓扑结构

1. 基本配置思路分析

本示例主要是 Totally Stub 区域的配置，所涉及的主要配置如下。

① 配置 Area1 为 Stub 区域（需要在 Area1 内所有的路由器上配置）。

② 在 RouterA 上配置禁止向 Stub 区域通告 Type3 LSA，使 Area1 成为 Totally Stub 区域，以进一步减少向区域内通告的 LSA。

③ 在 RouterD 上配置静态路由，并在 OSPF 进程中引入，以此来验证当把 Area1 配置为 Totally Stub 区域后，区域内的各部路由器的 OSPF 路由表中不能见到所引入的外部路由。

当然，在配置 Totally Stub 区域之前，还需要在各路由器上使能 OSPF，配置 OSPF 基本功能。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口 IP 地址为例进行介绍，RouterB、RouterC、RouterD、RouterE 和 RouterF 的配置方法一样，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.0.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

② 在整个 OSP 网络中的各路由器上配置 OSPF 基本功能，实现 OSPF 路由互通。均采用缺省的 OSPF 进程 1，所以在创建进程时不用写具体的进程号。假设示例中各路由器没有再连接除已标识的网段外的其他网段。

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
```

```
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit
[RouterB] router id 2.2.2.2

[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] area 2
[RouterB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.2] quit

[RouterC] router id 3.3.3.3
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] quit
[RouterD] router id 4.4.4.4

[RouterD] ospf
[RouterD-ospf-1] area 2
[RouterD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.2] quit

[RouterE] router id 5.5.5.5
[RouterE] ospf
[RouterE-ospf-1] area 1
[RouterE-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.1] quit

[RouterF] router id 6.6.6.6
[RouterF] ospf
[RouterF-ospf-1] area 2
[RouterF-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[RouterF-ospf-1-area-0.0.0.2] quit
```

③ 在 RouterD 上配置一条到达 200.0.0.0/8 的“黑洞”（以 NULL0 接口为出接口）静态路由，使到达 200.0.0.0/8 网络的报文均直接丢弃，并在 OSPF 1 进程中引入。此处对于本示例来说没什么意义，只是用来说明下面在把 Area1 配置为 Totally Stub 区域后，该区域内各路由器上见不到由 OSPF 引入的这条外部静态路由。

```
[RouterD] ip route-static 200.0.0.0 8 null 0
[RouterD] ospf
[RouterD-ospf-1] import-route static type 1
[RouterD-ospf-1] quit
```

此时可通过 **display ospf abr-asbr** 命令查看 RouterC 的 ABR/ASBR 信息，可以看到 RouterA 为 ABR，RouterD 为 ASBR。

```
[RouterC] display ospf abr-asbr
          OSPF Process 1 with Router ID 3.3.3.3
```

```
                    Routing Table to ABR and ASBR
 RtType        Destination      Area        Cost    Nexthop          Type
 Intra-area    1.1.1.1          0.0.0.1     1       192.168.1.1      ABR
 Inter-area    4.4.4.4          0.0.0.1     3       192.168.1.1      ASBR
```

再通过 **display ospf routing** 命令查看 RouterC 的 OSPF 路由表。此时当 RouterC 所在区域 Area1 作为普通区域时，可以看到路由表中存在 AS 外部的路由，即前面在 RouterD 上引入的静态路由（**参见输出信息中的粗体字部分**），其他路由器的 OSPF 路由表中也可见。

```
[RouterC] display ospf routing
     OSPF Process 1 with Router ID 3.3.3.3
                  Routing Tables
 Routing for Network
 Destination        Cost  Type         NextHop          AdvRouter       Area
 172.16.1.0/24      1     Transit      172.16.1.1       3.3.3.3         0.0.0.1
 172.17.1.0/24      4     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 192.168.0.0/24     2     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 192.168.1.0/24     1     Transit      192.168.1.2      3.3.3.3         0.0.0.1
 192.168.2.0/24     3     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 Routing for ASEs
 Destination     Cost     Type       Tag        NextHop          AdvRouter
 200.0.0.0/8     4        Type1      1          192.168.1.1      4.4.4.4
 Total Nets: 6
 Intra Area: 2   Inter Area: 3   ASE: 1   NSSA: 0
```

④ 现在来配置 Area1 为 Stub 区域，**需要在区域内各路由器上配置**。下面仅以 RouterA 上的配置为例进行介绍，其他路由器的配置一样，略。

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] stub
[RouterA-ospf-1-area-0.0.0.1] quit
```

现在再通过 **display ospf routing** 命令查看 RouterC 的 OSPF 路由表。此时可以发现，当把 RouterC 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条缺省路由（**参见输出信息中的粗体字部分**）。

```
[RouterC] display ospf routing
          OSPF Process 1 with Router ID 3.3.3.3
                  Routing Tables
 Routing for Network
 Destination        Cost  Type         NextHop          AdvRouter       Area
 0.0.0.0/0          2     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 172.16.1.0/24      1     Transit      172.16.1.1       3.3.3.3         0.0.0.1
 172.17.1.0/24      4     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 192.168.0.0/24     2     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 192.168.1.0/24     1     Transit      192.168.1.2      3.3.3.3         0.0.0.1
 192.168.2.0/24     3     Inter-area   192.168.1.1      1.1.1.1         0.0.0.1
 Total Nets: 6
 Intra Area: 2   Inter Area: 4   ASE: 0   NSSA: 0
```

⑤ 再在 Area1 的 ABR——RouterA 上配置禁止向 Stub 区域通告 Type3 LSA，把 Area1 配置成 Totally Stub 区域。

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] stub no-summary
[RouterA-ospf-1-area-0.0.0.1] quit
```

此时可再通过 **display ospf routing** 命令查看 RouterC 的 OSPF 路由表。从中可以看出，禁止向 Stub 区域通告 Summary LSA 后，Stub 路由器的路由表项进一步减少，凡是区域间的路由都没有了，只保留了一条通往区域外部的缺省路由（**参见输出信息中的粗体字部分**）。

```
[RouterC] display ospf routing
        OSPF Process 1 with Router ID 3.3.3.3
                Routing Tables
 Routing for Network
 Destination      Cost  Type        NextHop         AdvRouter       Area
 0.0.0.0/0        2     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 172.16.1.0/24    1     Transit     172.16.1.1      3.3.3.3         0.0.0.1
 192.168.1.0/24   1     Transit     192.168.1.2     3.3.3.3         0.0.0.1
 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

通过以上步骤就完成了本示例的全部配置，并且证明配置是成功的。

12.7.5　OSPF 的 NSSA 区域配置示例

本示例的基本拓扑结构如图 12-25 所示，所有的路由器都运行 OSPF，整个自治系统划分为两个区域。其中 RouterA 和 RouterB 作为 ABR，用来转发区域之间的路由，RouterD 作为 ASBR 引入了外部路由（这里也以静态路由为例）。现要求将 Area1 配置为 NSSA 区域。配置 NSSA 区域中的 RouterA 和 RouterB 为转换路由器，配置 RouterD 为引入外部路由（静态路由）的 ASBR，且路由信息可正确地在 AS 内传播。

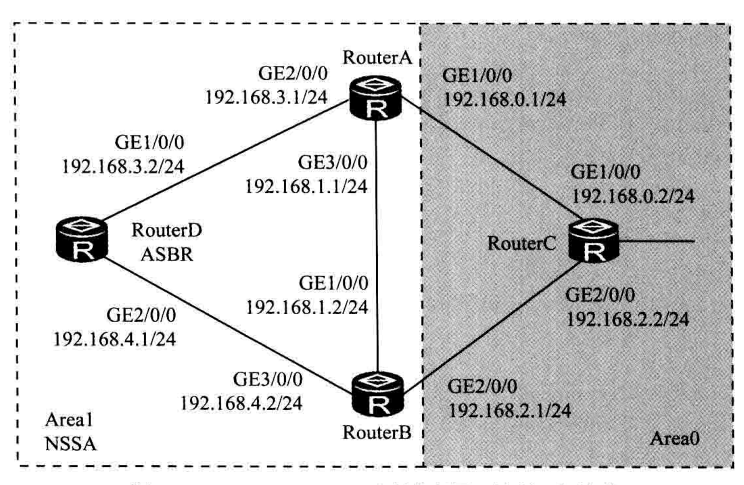


图 12-25　OSPF NSSA 区域配置示例拓扑结构

1. *基本配置思路分析*

本示例主要是 NSSA 区域的配置，所涉及的主要配置如下。

① 配置 Area1 为 NSSA 区域（需要在 Area1 内所有的路由器上配置）。

② 在 RouterD 上配置静态路由，并在 OSPF 进程中引入，以此来验证当把 Area1 配置为 NSSA 区域后各区域内部路由器的 OSPF 路由表中可见到所引入的外部路由。

③ 配置 RouterA 作为 NSSA 区域中的转换路由器，使 NSSA 区域中引入的外部路由转换通过 RouterA 向其他区域中的路由器（如本示例中的 RouterC）进行通告，验证

转换器的配置。

当然，在配置 NSSA 区域之前，还需要在各路由器上使能 OSPF，并配置 OSPF 基本功能。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口 IP 地址为例进行介绍，RouterB、RouterC 和 RouterD 的配置方法一样，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.0.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.3.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

② 配置 OSPF 基本功能，实现 OSPF 路由互通，也是均采用缺省的 OSPF 进程 1，所以在创建进程时不用写具体的进程号。假设示例中各路由器没有再连接除已标识的网段外的其他网段。

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] network 192.168.3.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit

[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.2] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.2] network 192.168.4.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.2] quit

[RouterC] router id 3.3.3.3
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.1] network 192.168.0.0 0.0.255.255
[RouterC-ospf-1-area-0.0.0.1] quit

[RouterD] router id 4.4.4.4
[RouterD] ospf
[RouterD-ospf-1] area 1
[RouterD-ospf-1-area-0.0.0.2] network 192.168.0.0 0.0.255.255
[RouterD-ospf-1-area-0.0.0.2] quit
```

③ 在各路由器上配置 Area1 区域为 NSSA 区域。下面仅以 RouterA 上的配置为例进行介绍，其他路由器的配置一样，略。

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] nssa
[RouterA-ospf-1-area-0.0.0.1] quit
```

④ 在 RouterD 上配置一条到达 100.0.0.0/8 的“黑洞”（以 NULL0 接口为出接口）静态路由，使到达 100.0.0.0/8 网络的报文均直接丢弃，并在 OSPF 1 进程中引入。这里也仅用于证明下面将要介绍的 NSSA 区域可以引入自己 ASBR 所引入的外部路由。

```
[RouterD] ip route-static 100.0.0.0 8 null 0
[RouterD] ospf
[RouterD-ospf-1] import-route static
[RouterD-ospf-1] quit
```

此时可通过 **display ospf routing** 命令查看 RouterC 的 OSPF 路由表。可以看到 NSSA 区域引入的 AS 外部路由的发布路由器的路由器 ID 为 2.2.2.2（**参见输出信息中的粗体字部分**）。此时，虽然在 Area1 中有两个 ABR，但 OSPF 会选举 Router ID 较大的 ABR 作为转换路由器，所以最终的转换器是 RouterB。

```
[RouterC] display ospf routing

          OSPF Process 1 with Router ID 3.3.3.3
                   Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.3.0/24     2     Inter-area 192.168.0.1     1.1.1.1         0.0.0.0
 192.168.4.0/24     2     Inter-area 192.168.2.1     2.2.2.2         0.0.0.0
 192.168.0.0/24     1     Transit    192.168.0.2     3.3.3.3         0.0.0.0
 192.168.1.0/24     2     Inter-area 192.168.0.1     1.1.1.1         0.0.0.0
 192.168.1.0/24     2     Inter-area 192.168.2.1     2.2.2.2         0.0.0.0
 192.168.2.0/24     1     Transit    192.168.2.2     3.3.3.3         0.0.0.0

 Routing for ASEs
 Destination        Cost      Type       Tag       NextHop         AdvRouter
 100.0.0.0/8        1         Type2      1         192.168.2.1     2.2.2.2

 Total Nets: 7
 Intra Area: 2  Inter Area: 4  ASE: 1  NSSA: 0
```

通过 **display ospf lsdb** 命令查看 RouterC 的 OSPF LSDB，可以看到所引入的外部 LSA（**参见输出信息中的粗体字部分**）。

```
[RouterC] display ospf lsdb

          OSPF Process 1 with Router ID 3.3.3.3
                  Link State Database

                          Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    3.3.3.3         3.3.3.3            345  72    80000004     1
 Router    2.2.2.2         2.2.2.2            346  48    80000005     1
 Router    1.1.1.1         1.1.1.1            193  48    80000006     1
 Network   192.168.0.2     3.3.3.3            385  32    80000007     0
```

```
Network    192.168.2.2    3.3.3.3     387  32    80000008      0
Sum-Net    192.168.4.0    2.2.2.2     393  28    80000001      1
Sum-Net    192.168.4.0    1.1.1.1     189  28    80000001      2
Sum-Net    192.168.3.0    1.1.1.1     189  28    80000002      1
Sum-Net    192.168.3.0    2.2.2.2     192  28    80000002      2
Sum-Net    192.168.1.0    2.2.2.2     393  28    80000001      1
Sum-Net    192.168.1.0    1.1.1.1     189  28    80000002      1

                 AS External Database
Type       LinkState ID   AdvRouter       Age  Len   Sequence   Metric
External   100.0.0.0      2.2.2.2         257  36    80000002     1
```

⑤ 配置 RouterA 为转换路由器。

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary translator-always
[RouterA-ospf-1-area-0.0.0.1] quit
[RouterA-ospf-1] quit
```

再在 RouterC 上通过 **display ospf routing** 命令查看 OSPF 路由表。此时，可以看到 NSSA 区域引入的 AS 外部的路由的发布路由器的 Router ID 变为 1.1.1.1，即 RouterA 成为了转换路由器（**参见输出信息中的粗体字部分**）。

```
[RouterC] display ospf routing

          OSPF Process 1 with Router ID 3.3.3.3
                   Routing Tables
Routing for Network
Destination          Cost  Type          NextHop       AdvRouter      Area
192.168.3.0/24       2     Inter-area 192.168.0.1    1.1.1.1        0.0.0.0
192.168.4.0/24       2     Inter-area 192.168.2.1    2.2.2.2        0.0.0.0
192.168.0.0/24       1     Transit       192.168.0.2   3.3.3.3        0.0.0.0
192.168.1.0/24       2     Inter-area 192.168.2.1    2.2.2.2        0.0.0.0
192.168.1.0/24       2     Inter-area 192.168.0.1    1.1.1.1        0.0.0.0
192.168.2.0/24       1     Transit       192.168.2.2   3.3.3.3        0.0.0.0

Routing for ASEs
Destination          Cost      Type      Tag    NextHop        AdvRouter
100.0.0.0/8          1         Type2     1      192.168.0.1    1.1.1.1

Total Nets: 7
Intra Area: 2   Inter Area: 4   ASE: 1   NSSA: 0
```

说明 缺省情况下，新指定的转换路由器会和以前的转换路由器共同承担 40 s 转换路由器的角色，过了 40 s 后，新指定的转换路由器会继续独立完成转换路由器的工作。

如果再在 RouterC 上通过 **display ospf lsdb** 命令查看 OSPF LSDB，此时，同样可以发现外部 LSA 也是通过 RouterA 来进行通告（**参见输出信息中的粗体字部分**）。

```
[RouterC] display ospf lsdb

          OSPF Process 1 with Router ID 3.3.3.3
                 Link State Database

                         Area: 0.0.0.0
Type       LinkState ID   AdvRouter       Age  Len   Sequence   Metric
Router     3.3.3.3        3.3.3.3         493  72    80000004     1
```

```
Router    2.2.2.2       2.2.2.2     494  48   80000005    1
Router    1.1.1.1       1.1.1.1     341  48   80000006    1
Network   192.168.0.2   3.3.3.3     501  32   80000007    0
Network   192.168.2.2   3.3.3.3     503  32   80000008    0
Sum-Net   192.168.4.0   2.2.2.2     541  28   80000001    1
Sum-Net   192.168.4.0   1.1.1.1     337  28   80000001    2
Sum-Net   192.168.3.0   1.1.1.1     337  28   80000002    1
Sum-Net   192.168.3.0   2.2.2.2     340  28   80000002    2
Sum-Net   192.168.1.0   2.2.2.2     541  28   80000001    1
Sum-Net   192.168.1.0   1.1.1.1     337  28   80000002    1

              AS External Database
Type      LinkState ID  AdvRouter   Age  Len  Sequence    Metric
External  100.0.0.0     1.1.1.1     248  36   80000001    1
```

通过以上步骤就完成了本示例的全部配置，并且证明配置是成功的。

12.8　配置 OSPF 安全功能

在对安全性要求较高的网络中，可以通过配置 GTSM（Generalized TTL Security Mechanism，通用 TTL 安全保护机制）以及 OSPF 区域认证和接口认证来提高 OSPF 网络的安全性。但在配置这些 OSPF 安全功能之前，需完成以下配置任务。

① 配置接口的网络层地址，使各相邻节点网络层可达。

② 配置 OSPF 的基本功能。

12.8.1　配置 OSPF GSTM 功能

如果攻击者模拟真实的 OSPF 协议单播报文，对一台路由器不断地发送报文，而路由器接口板在收到这些报文后，发现目的 IP 地址是本设备的接口地址，则会直接上送给控制层面的 OSPF 协议处理，不辨别其“合法性”，这样就会导致路由器控制层面因为忙于处理这些假合法的报文使系统异常繁忙，占用较多的 CPU 资源。此时，可通过 GTSM 检查 IP 报文头中的 TTL 值是否在一个预先定义好的范围内，对 IP 层以上业务进行保护。**但 GTSM 仅对单播报文有效，对组播报文无效**，这是因为组播报文本身具有 TTL 值为 255 的限制，不需要使用 GTSM 进行保护。**同时，GTSM 不支持基于 Tunnel 的邻居。**

GTSM 的实现机制是：对于直连的协议邻居，将需要发出的单播协议报文的 TTL 值设定为 255；而对于多跳的邻居则可以定义一个合理的 TTL 范围。使能了 GTSM 特性和策略的设备会对收到的所有 IP 单播报文进行策略检查，对于没有通过策略的报文丢弃或者上送控制平面，从而达到防止攻击的目的。GSTM 的策略内容主要包括以下几种。

① 发送给本机 IP 报文的源地址。

② 报文所属的 VPN 实例。

③ IP 报文的协议号（OSPF 是 89，BGP 是 6）。

④ TCP/UDP 之上协议的协议源端口号、目的端口号。

⑤ 有效 TTL 范围（**OSPFv2 版本中仅支持这一策略**）。

应用 GTSM 功能，需要在 OSPF 连接的两端都使能 GTSM。被检测的报文的 TTL

值有效范围为 [255−*hops*+1, 255]。GTSM 只会对匹配 GTSM 策略的报文进行 TTL 检查。对于未匹配策略的报文，可以设置为通过或丢弃。如果配置 GTSM 缺省报文动作为丢弃，就需要在 GTSM 中配置所有可能的路由器连接情况，没有配置的路由器发送的报文将被丢弃，无法建立连接。因此，在保证安全性的同时会损失一些易用性。对于丢弃的报文，可以通过 Log 信息开关控制是否对报文被丢弃的情况记录日志。记录日志有助于用户在需要时进行故障定位。

OSPF GTSM 功能的主要配置任务包括以下几种。

① 使能 GTSM 功能。

②（可选）配置未匹配 GSTM 策略的报文处理动作。

③（可选）配置日志功能。

这三项配置任务的具体配置步骤如表 12-12 所示。

表 12-12　　OSPF GTSM 功能的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf valid-ttl-hops** *hops* [**vpn-instance** *vpn-instance-name*] 例如：[Huawei] **ospf valid-ttl-hops** 5	使能 OSPF GTSM 特性，并配置需要检测 TTL 值的 GTSM 策略。命令中的参数说明如下 ● *hops*：指定需要检测的最大 TTL 值，取值范围为 1～255 的整数，缺省值为 255 ● **vpn-instance** *vpn-instance-name*：可选参数，指定使能 GSTM 特性的 VPN 实例的名称，1～31 个字符，区分大小写，不支持空格。如果不指定此参数，则将同时在公网和私网中使能 OSPF GTSM 特性 【说明】GTSM 只会对匹配 GTSM 策略的报文进行 TTL 检查，而对于未匹配策略的报文，可以通过下面第 3 步中的 **gtsm default-action** 命令的参数 pass 通过报文或 drop 丢弃报文 缺省情况下，没有使能 OSPF GTSM 特性，可用 **undo ospf valid-ttl-hops** [*hops*] [**vpn-instance** *vpn-instance-name*] 命令删除相应的 OSPF GTSM 特性
3	**gtsm default-action** { **drop** | **pass** } 例如：[Huawei] **gtsm default-action drop**	（可选）设置未匹配 GTSM 策略的报文的缺省动作是丢弃（选择二选一选项 drop 时），还是通过（选择二选一选项 **pass** 时）。如果配置 GTSM 缺省报文动作为丢弃，路由器可能无法建立连接 【说明】对于丢弃的报文，可以通过下面第 4 步的 **gtsm log drop-packet** 命令打开 LOG 信息开关，对报文被丢弃的情况记录日志，以便进行故障定位 缺省情况下，未匹配 GTSM 策略的报文可以通过过滤，可用 **undo gtsm default-action drop** 命令取消未匹配 GTSM 策略的报文不能通过过滤的设置
4	**gtsm log drop-packet all** 例如：[Huawei]**gtsm log drop-packet all**	（可选）打开所有单板的 Log 信息开关，在单板 GTSM 丢弃报文时记录 Log 信息。仅当上一步通过 **gtsm default-action drop** 命令设置丢弃（**drop**）报文时才有效 缺省情况下，在单板 GTSM 丢弃报文时不记录 Log 信息，可用 **undo gtsm log drop-packet all** 命令关闭所有单板 Log 信息的开关

12.8.2　配置 OSPF 安全认证功能

为了拒绝非法 OSPF 报文进入，OSPF 支持报文认证功能，使只有通过认证的 OSPF 报文才能被接收，否则将不能正常建立邻居。路由器支持两种认证方式：①区域认证方式；②接口认证方式。**使用区域认证时，一个区域中所有的路由器在该区域下的认证模式和密码必须一致。**

OSPF 区域和接口认证的具体配置步骤如表 12-13 所示（可仅采用一种配置方式，也可同时配置，**但如果同时配置了两种认证方式，则优先使用接口认证方式**）。

表 12-13　OSPF 区域和接口认证的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	配置区域认证方式	
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	键入要配置区域认证的 OSPF 进程，进入 OSPF 视图
3	**area** *area-id* 例如：[Huawei-ospf-10] **area** 1	键入要配置区域认证的区域 ID，进入区域视图
4	**authentication-mode simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] 例如：[Huawei-ospf-10-area-0.0.0.1] **authentication-mode simple cipher** huawei	（三选一）配置 OSPF 区域的简单认证模式。命令中的参数和选项说明如下 ● **plain** *plain-text*：二选一参数，指定简单认证的明文密码，1～8 个字符，可以为字母或数字，区分大小写，不支持空格。此模式下只能键入明文密码，密码将以明文形式保存在配置文件中 ● **cipher**：可选项，指定为密文密码，此时可以键入明文或密文密码，但在查看配置文件时是以密文方式显示的 ● *cipher-text*：二选一参数，指定简单认证的密文密码，可以为字母或数字，区分大小写，不支持空格，长度为 1～8 位明文密码或 32 位密文密码 缺省情况下，没有配置区域认证模式，可用 **undo authentication-mode** 命令取消对应区域已配置的认证模式
	authentication-mode { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] 例如：[Huawei-ospf-10-area-0.0.0.1] **authentication-mode md5** 1 **cipher** huawei	（三选一）配置 OSPF 区域的 **md5** 或 **hmac-md5** 或 **hmac-sha256** 认证模式。命令中的参数和选项说明如下 ● **md5**：多选一选项，指定使用 MD5 密文认证模式 ● **hmac-md5**：多选一选项，指定使用 HMAC MD5 密文认证模式 ● **hmac-sha256**：多选一选项，使用 HMAC-SHA256 密文认证模式 ● *key-id*：可选参数，指定密文认证的认证密钥标识符，取值范围为 1～255 的整数，必须与对端的认证密钥标识符一致 ● **plain** *plain-text*：二选一可选参数，指定认证的明文密码，1～255 个字符，可以为字母或数字，区分大小写，不支持空格。此模式下只能键入明文密码，密码将以明文形式保存在配置文件中 ● **cipher**：可选项，指定为密文密码，此时可以键入明文或密文密码，但在查看配置文件时是以密文方式显示的

（续表）

步骤	命令	说明
4	**authentication-mode** { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] 例如：[Huawei-ospf-10-area-0.0.0.1] **authentication-mode md5** 1 **cipher** huawei	• *cipher-text*：二选一可选参数，指定简单认证的密文密码，可以为字母或数字，区分大小写，不支持空格，长度为1～255 位明文密码或 20～392 位密文密码 缺省情况下，没有配置区域认证模式，可用 **undo authentication-mode** 命令取消对应区域已配置的认证模式
	authentication-mode keychain *keychain-name* 例如：[Huawei-ospf-10-area-0.0.0.1] **authentication-mode keychain** areachain	（三选一）配置 OSPF 区域的 Keychain 认证模式，参数 *keychain-name* 用来指定 Keychain 名称，1～47 个字符，不区分大小写，不支持空格 【说明】所使用的 Keychain（密钥链）需已使用 **keychain** *keychain-name* 命令创建，然后分别通过 **key-id** *key-id*、**key-string** { [**plain**] *plain-text* | [**cipher**] *cipher-text* }和 **algorithm** { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }命令配置该 keychain 采用的 key-id、密码及其认证算法，必须保证本端和对端的 key-id、algorithm、key-string 相同，才能建立 OSPF 邻居 缺省情况下，没有配置区域认证模式，可用 **undo authentication-mode** 命令取消对应区域已配置的认证模式
配置接口认证方式		
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置接口认证的 OSPF 接口，进入接口视图
3	**ospf authentication-mode simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] 例如：[Huawei-GigabitEthernet1/0/0] **ospf authentication-mode simple cipher** huawei	（三选一）配置 OSPF 接口的简单认证模式，命令中的参数和选项说明参见本表前面介绍的区域简单认证方式 缺省情况下，接口不对 OSPF 报文进行认证，可用 **undo ospf authentication-mode** 命令删除接口下已设置的认证模式
	ospf authentication-mode { **md5** | **hmac-md5** | **hmac-sha256**} [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] 例如：[Huawei-GigabitEthernet1/0/0] **ospf authentication-mode md5** 1 **cipher** huawei	（三选一）配置 OSPF 接口的 **md5** 或 **hmac-md5** 或 **hmac-sha256** 认证模式，命令中的参数和选项说明参见本表前面介绍的区域 **md5** 或 **hmac-md5** 或 **hmac-sha256** 认证方式 缺省情况下，接口不对 OSPF 报文进行认证，可用 **undo ospf authentication-mode** 命令删除接口下已设置的认证模式
	ospf authentication-mode keychain *keychain-name* 例如：[Huawei-GigabitEthernet1/0/0] **ospf authentication-mode keychain** areachain	（三选一）配置 OSPF 接口的 Keychain 认证模式，命令中的参数及其他说明参见本表前面介绍的区域 Keychain 认证方式 缺省情况下，接口不对 OSPF 报文进行认证，可用 **undo ospf authentication-mode** 命令删除接口下已设置的认证模式

12.9 调整 OSPF 的路由选择

在复杂网络环境中，可通过调整 OSPF 的功能参数来达到灵活组网、优化网络负载分担。可根据具体应用环境选择以下一项或几项任务进行配置。

① 配置 OSPF 的接口开销。
② 配置等价路由。
③ 配置 OSPF 路由选择规则。
④ 抑制接口接收和发送 OSPF 报文。

但在调整 OSPF 的选路之前，也需要先配置接口的网络层地址，使各相邻节点网络层可达，同时要配置 OSPF 的基本功能。

12.9.1 配置 OSPF 的接口开销

OSPF 接口开销值影响路由的选择，开销值越大，优先级越低。OSPF 既可以根据接口的带宽自动计算其链路开销值，也可以通过命令固定配置。根据该接口的带宽自动计算开销值的公式为：接口开销=带宽参考值/接口带宽，取计算结果的整数部分作为接口开销值（当结果小于 1 时取 1），通过改变带宽参考值可以间接改变接口的开销值。这样一来，就可以有两种方式来调整 OSPF 的接口开销：一是直接配置接口的开销值；二是通过改变带宽参考值调整接口开销值。这两种方法的具体配置步骤如表 12-14 所示。

【经验之谈】链路状态路由协议（包括 **OSPF** 和 **IS-IS** 协议）的接口开销也即链路开销，是二层概念，是指接口所在链路的开销，主要依据接口带宽确定，具体将在本节后面介绍。如果链路两端接口带宽不一致，则以带宽低的接口为准计算接口开销。路由开销等于所经过的链路开销之和，但同一路由器上的不同接口之间的链路开销为 0。

表 12-14　OSPF 接口开销的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
方式 1：直接配置方法		
2	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要配置 OSPF 开销的接口，进入接口视图
3	**ospf cost** *cost* [Huawei-GigabitEthernet1/0/0] **ospf cost** 65	直接配置接口的 OSPF 开销，取值范围为 1～65 535 的整数，缺省值是 1 缺省情况下，OSPF 会根据该接口的带宽自动计算其开销值。计算公式为：接口开销＝带宽参考值/接口带宽，取计算结果的整数部分作为接口开销值(当结果小于 1 时取 1)。缺省情况下，OSPF 的带宽参考值为 100 Mbit/s，根据以上公式可以得到一些主要类型的接口缺省开销值如下 • 56 kbit/s 串口：1 785 • 64 kbit/s 串口：1 562 • E1（2.048 Mbit/s)：48 • Ethernet（100 Mbit/s)：1 • GigabitEthernet（1 000 Mbit/s)：1 可用 **undo ospf cost** 命令恢复接口上运行 OSPF 所需开销的缺省值 【说明】由于 Eth-Trunk 接口开销是各个成员接口开销的总和，并且各个成员接口是变化的，所以 Eth-Trunk 接口没有缺省的接口开销值

（续表）

步骤	命令	说明
方式 2：通过改变带宽参考值间接调整接口开销的方法		
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
3	**bandwidth-reference** *value* 例如：[Huawei-ospf-10] **bandwidth-reference 1000**	设置通过公式计算接口开销所依据的带宽参考值，取值范围为（1～2 147 483 648）Mbit/s。配置成功后，进程内所有接口的带宽参考值都会改变，**必须保证该进程中所有路由器的带宽参考值一致** 【说明】本命令对于 Eth-Trunk 接口的处理方式同物理接口一样，但接口带宽等于该接口绑定的所有成员接口的带宽之和 缺省情况下，带宽参考值为 100 Mbit/s，可用 **undo bandwidth-reference** 命令恢复带宽参考值为缺省值

12.9.2 配置等价路由

当网络中存在多条由相同路由协议发现的到达同一目的地的路由，且这几条路由的开销值也相同时，则这些路由就是等价路由，就可以实现负载分担。

例如，如图 12-26 所示，路由器 A 和路由器 B 之间的三条路由都运行 OSPF 协议，且几条路由的开销值也相同（均为 15），那么这三条路由就是等价路由，形成了负载分担。

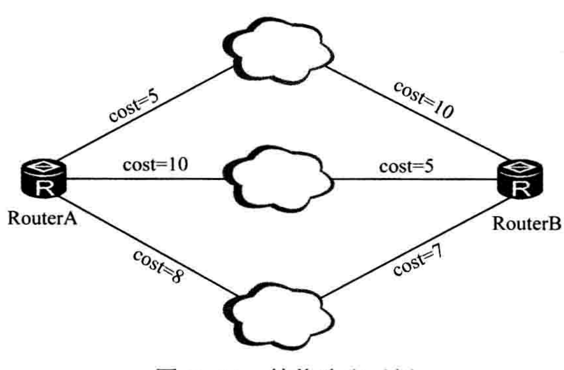


图 12-26　等价路由示例

在 OSPF 中可以配置最大的等价路由条数，具体的配置步骤很简单，如表 12-15 所示。

表 12-15　　OSPF 等价路由的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图

（续表）

步骤	命令	说明
3	**maximum load-balancing** *number* 例如：[Huawei-ospf-10] **maximum load-balancing** 2	配置最大等价路由数量，但不同 AR G3 系列所的取值范围不一样：AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2201-48FE/AR2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 的取值范围为 1～4 的整数，AR2220、AR2220L、AR2240/2240-S 和 AR3200 系列的取值范围为 1～8 的整数 缺省情况下，AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2201-48FE/AR2201-48FE-S、AR2202-48FE 和 AR2204/2204-S 负载分担方式下的最大等价路由的数量为 4，AR2220、AR2220L、AR2240/2240-S 和 AR3200 系列负载分担方式下的最大等价路由的数量为 8，可用 **undo maximum load-balancing** 命令恢复等价路由的最大数量为缺省值
4	**nexthop** *ip-address* **weight** *value* 例如：[Huawei-ospf-10] **nexthop** 10.0.0.3 **weight** 1	（可选）配置 OSPF 的负载分担优先级。如果网络中存在的等价路由数量大于在上一步配置的最大等价路由数量时，则可以通过本命令配置路由的优先级，指定是哪些等价路由可以用于负载分担（**依次按优先级高低进行选择**）。命令中的参数说明如下 ● *ip-address*：指定要配置路由优先级的某条等价路由的下一跳 IP 地址 ● *value*：指定由参数 *ip-address* 指定的路由的优先级，取值范围是 1～254 的整数，值越小，路由优先级越高 缺省情况下，weight 的取值是 255（最低），即各等价路由间没有优先级高低之分，同时转发报文，进行负载分担，可用 **undo nexthop** *ip-address* 命令取消对应下一跳的等价路由的优先级设置 【说明】如果网络中的流量比较小，则可能不会有最大数量的等价路由进行负载分担，这时也是依据本命令配置的路由优先级取消一些路由的负载分担的，优先级越低的越先取消，最小可以仅靠一条优先级最高的路由在承载负载流量

12.9.3　配置 OSPF 路由选择规则

OSPFv2 在发展过程中，经过了几次大的修改，其中影响最大的就是 RFC1583 和 RFC2328 这两个修订版（目前最新的版本就是 RFC2328，本章也是按照这个版本进行介绍的）。在这两个版本中，在计算外部路由时的规则不一样，可能会导致路由环路。它们各自的外部路由计算规则比较复杂，在此就不作具体介绍。为了避免路由环路的发生，在最新的 RFC2328 中提出了 RFC1583 兼容特性，使能 RFC1583 兼容特性后，OSPF 采用 RFC1583 的路由计算规则。

OSPF 路由选择规则的配置很简单，仅需在对应的 OSPF 进程视图下通过 **rfc1583 compatible** 命令配置即可。缺省情况下，OSPF 支持 RFC1583 定义的规则，但如果 OSPF 域的其他设备配置的都是 RFC2328 选路规则，则需要通过 **undo rfc1583 compatible** 命令配置成 RFC2328 定义的选路规则。

【示例】配置将 RFC1583 定义的规则配置成 RFC2328 定义的规则，即不再兼容 RFC1583。

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] undo rfc1583 compatible
```

12.9.4 抑制接口接收和发送 OSPF 报文

通过抑制接口接收和发送的 OSPF 报文，使路由信息不被某一网络中的路由器获得，且使本地路由器不接收网络中其他路由器发布的路由更新信息，从而达到优先保证某条路由的目的。如本地路由器有一条到达某个目的地的路由，但通过其他区域的路由通告，或者引入外部路由，可能还有其他更佳的路由到达同一目的地。这时为了使本路由器上的这条路由最终生效，就可以配置对应接口为抑制状态。

配置抑制接口接收和发送 OSPF 报文的方法就是在对应的 OSPF 进程视图下通过 **silent-interface** { **all** | *interface-type interface-number* } 命令把本地路由器上的所有接口（选择二选一选项 all 时）或者指定接口（选择二选一参数 *interface-type interface-number* 时）**（除了可以是物理接口外，还可以是像 VLANIF 和 Eth-Trunk 等之类的逻辑接口）**配置为静默接口。

将运行 OSPF 协议的接口指定为 Silent 状态后，**该接口的直连路由仍可以通过 OSPF 协议发布出去，但接口的 Hello 报文发送和接收都将被阻塞，接口上无法与其他设备建立邻居关系**，其他 OSPF 报文就更无法发送和接收了。这样可以增强 OSPF 的组网适应能力，减少系统资源的消耗。但本命令仅对本进程已经使能的 OSPF 接口起作用，对其他进程的接口不起作用。

【示例】在 OSPF 100 进程下禁止 VLANIF200 接口收发 OSPF 报文。

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] silent-interface vlanif 200
```

12.10 控制 OSPF 路由信息的发布和接收

控制 OSPF 路由信息的发布和接收包括外部路由引入控制，缺省路由通告控制，路由聚合控制和路由、LSA 的发布或接收过滤。具体可以根据应用环境选择其中一项或几项任务进行配置。

① 配置 OSPF 引入外部路由。

② 配置 OSPF 将缺省路由通告到 OSPF 区域。

③ 配置 OSPF 路由聚合。

④ 配置 OSPF 对接收和发布的路由进行过滤。

⑤ 配置对发送的 LSA 进行过滤。

⑥ 配置对 ABR Type3 LSA 进行过滤。

但在控制 OSPF 的路由信息之前，也要先配置接口的网络层地址，使各相邻节点网

络层可达；配置 OSPF 的基本功能。

12.10.1　配置 OSPF 引入外部路由

当 OSPF 网络中的设备需要访问运行其他协议的网络中的设备时，需要将其他协议的路由引入 OSPF 进程中，但这**仅可以在连接了其他 AS 的 ASBR 上进行配置**。

注意 尽管 OSPF 是一个无环路的动态路由协议，但这是针对域内路由和域间路由而言的，其对引入的外部路由环路没有很好的防范机制，所以在配置 OSPF 引入外部路由时一定要慎重，防止手动配置引起的环路。

在 OSPF ASBR 上配置引入外部路由的步骤如表 12-16 所示（**仅针对引入非缺省路由**）。

表 12-16　OSPF ASBR 引入外部路由的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
3	**import-route** { **limit** *limit-number* | { **bgp** [**permit-ibgp**] | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf**[*process-id-ospf*] } [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * } 例如：[Huawei-ospf-10] **import-route rip** 40 **type** 2 **tag** 33 **cost** 50 （引入 RIP 进程 40 的路由，并设置外部路由类型为 Type 2，路由标记为 33，开销值为 50）	引入其他路由协议学习到的**非缺省路由信息**。命令中的参数和选项说明如下 ● **limit** *limit-number*：二选一参数，指定在一个 OSPF 进程中可引入的最大外部路由数量，取值范围为 1～4 294 967 295 的整数 ● **bgp**：多选一选项，指定引入 BGP 路由 ● **permit-ibgp**：可选项，指定允许同时引入 IBGP 路由。但由于引入 IBGP 路由后可能导致路由环路，所以在非必要场合请不要选择 ● **direct**：多选一选项，指定引入直连路由 ● **unr**：多选一选项，指定引入 UNR（User Network Route，用户网络路由）。UNR 主要用于在用户上线过程中由于无法使用动态路由协议时给用户分配的路由 ● **rip**：多选一选项，指定引入 RIP 路由 ● *process-id-rip*：可多选参数，指定仅引入指定进程的 RIP 路由，取值范围为 1～65 535 的整数，缺省值是 1 ● **static**：多选一选项，指定引入静态路由 ● **isis**：多选一选项，指定引入 IS-IS 路由 ● *process-id-isis*：可多选参数，指定仅引入指定进程的 IS-IS 路由，取值范围为 1～65 535 的整数，缺省值是 1 ● **ospf**：多选一选项，指定引入 OSPF 路由 ● *process-id-ospf*：可多选参数，指定仅引入指定进程的 OSPF 路由，取值范围为 1～65 535 的整数，缺省值是 1 ● **cost** *cost*：可多选参数，指定引入后的外部路由开销值，取值范围为 0～16 777 214 的整数，缺省值是 1 ● **type** *type*：可多选参数，指定引入后的外部路由的类型，取值为 1（代表第一类外部路由）或 2（代表第二类外部路由），缺省值是 2 ● **tag** *tag*：可多选参数，指定引入后的外部路由的标记，取值范围为 0～4 294 967 295 的整数，缺省值是 1

（续表）

步骤	命令	说明
3	**import-route** { **limit** *limit-number* | { **bgp** [**permit-ibgp**] | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf**[*process-id-ospf*] } [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * } 例如：[Huawei-ospf-10] **import-route rip** 40 **type** 2 **tag** 33 **cost** 50 （引入 RIP 进程 40 的路由，并设置外部路由类型为 Type 2，路由标记为 33，开销值为 50）	• **route-policy** *route-policy-name*：可多选参数，只能引入符合指定路由策略的路由（相应的路由策略必须已创建）。**有关路由策略的详细介绍和配置方法参见本书第 15 章** 缺省情况下，不引入其他协议的路由信息，可用 **undo import-route** { **limit** | **bgp** | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf** [*process-id-ospf*] }命令删除指定引入的外部路由信息
4	**default** { **cost** { *cost-value* | **inherit-metric** } | **limit** *limit* | **tag** *tag* | **type** *type* } * 例如：[Huawei-ospf-10] **default cost** 10 **tag** 100 **type** 2	（可选）对于没有在上一步为引入的外部路由配置开销值、引入的路由条数、标记和外部路由类型等参数的外部路由，可以统一配置引入外部路由时的参数缺省。命令中的参数和选项说明如下 • **cost**：可多选选项，配置引入的外部路由的缺省开销 • *cost-value*：二选一参数，指定引入的外部路由的缺省度量值，取值范围是 0～16 777 214 的整数 • **inherit-metric**：二选一选项，指定引入路由的开销值为路由自带的开销值 • **limit** *limit*：可多选参数，指定单位时间内引入外部路由上限的缺省值，取值范围为 1～2 147 483 647 的整数 • **tag** *tag*：可多选参数，指定引入的外部路由的标记，取值范围为 0～4 294 967 295 的整数 • **type** *type*：可多选参数，指定引入的外部路由的缺省类型，取值为 1 或 2 缺省情况下，OSPF 引入外部路由的缺省度量值为 1，一次可引入外部路由数量的上限为 2 147 483 647，引入的外部路由类型为 Type2，缺省标记值为 1，可用 **undo default** { **cost** | **limit** | **tag** | **type** } *命令恢复各项为缺省值 【注意】设置引入路由的开销值有三种方法，其中采用本命令的方法优先级最低，仅作用于没有应用 **apply cost** [+ | −] *cost*（本命令的设置优先级最高）路由策略视图命令配置的外部路由，没有在本表第 3 步通过 **import-route**（**本命令的优先级次之**）引入外部路由时配置具体开销的外部路由

12.10.2 配置 OSPF 将缺省路由通告到 OSPF 区域

在 OSPF 实际组网应用中，区域边界和自治系统边界通常都是由多个路由器组成的多出口冗余备份或者负载分担。此时，为了减少路由表的容量，可以配置缺省路由来保证网络的高可用性。

OSPF 缺省路由通常应用于下面两种情况。

① 由 ABR 发布 Type3 LSA，用来指导区域内路由器进行区域之间报文的转发。

② 由 ASBR 发布 Type5 LSA 或 Type7 LSA，用来指导 OSPF 路由域内路由器进行域外报文的转发。

当路由器无精确匹配的路由时，就可以通过缺省路由进行报文转发。Type3 LSA 缺省路由的优先级要高于 Type5 LSA 或 Type7 LSA 路由。OSPF 缺省路由的发布方式取决于引入该缺省路由的区域类型，具体如表 12-17 所示。配置 OSPF 将缺省路由通告到 OSPF

路由区域的方法如表 12-18 所示，仅适用于运行了 OSPF 协议的 ASBR 上。

表 12-17 不同缺省路由的不同发布方式

区域类型	产生条件	发布方式	产生 LSA 的类型	泛洪范围
普通区域	通过 **default-route-advertise** 命令配置	ASBR 发布	Type5 LSA	普通区域
Stub 区域	自动产生	ABR 发布	Type3 LSA	Stub 区域
NSSA 区域	通过 **nssa** [**default-route-advertise**] 命令配置	ASBR 发布	Type7 LSA	NSSA 区域
完全 NSSA 区域	ABR 上自动产生，ABSR 上有缺省路由时产生	ABR 或者 ASBR 发布	Type3 LSA 或者 Type7 LSA	NSSA 区域

表 12-18 配置 OSPF 将缺省路由通告到 OSPF 路由区域的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
3	**default-route-advertise** [[**always** | **permit-calculate-other**] | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name* [**match-any**]] * 例如：[Huawei-ospf-10] **default-route-advertise always**	（可选）在 **ASBR** 上将缺省路由通告到 OSPF 路由区域。配置该命令后，ASBR 将产生一个 Link State ID 为 0.0.0.0，网络掩码为 0.0.0.0 的 ASE LSA（Type 5），并且通告到整个 OSPF 区域中。前面介绍的 **import-route** 命令不能引入外部路由的缺省路由（包括静态缺省路由）。命令中的参数和选项说明如下 • **always**：二选一可选项，指定无论本机是否存在激活的非 OSPF 缺省路由，OSPF 协议本身都将在整个区域中产生并通告一条 OSPF 缺省路由，**不再计算来自其他设备的缺省路由；如果不选择此可选项，则 OSPF 设备将不会生成缺省路由** • **permit-calculate-other**：二选一可选项，指定在 OSPF 发布自己的缺省路由后，**当本机存在激活的非 OSPF 缺省路由**时仍允许计算来自于其他设备的缺省路由。如果既没有选择 **permit-calculate-other** 可选项，也没有选择 **always** 可选项，不再计算来自其他设备的缺省路由，如果 ASBR 上已经有缺省路由，将在整个 OSPF 区域中通告该缺省路由 • **cost** *cost*：可多选参数，指定引入的外部缺省路由的开销值，取值范围为 0～16 777 214 的整数，缺省值是 1 • **type** *type*：可多选参数，指定引入的外部缺省路由的类型，取值为 1 或 2，缺省值是 2 • **route-policy** *route-policy-name*：可多选参数，指定仅当在路由表中有与指定名称的路由策略匹配的非 OSPF 产生的缺省路由表项时，按照指定的路由策略配置的参数发布缺省路由 • **match-any**：可选项，指定在 OSPF 路由表中有匹配的路由表项（不管是否是非 OSPF 产生的缺省路由表项）时就按路由策略所配置的参数发布缺省路由。如果有多条路由通过策略，选取最优者来生成缺省 LSA。选取最优者的原则按照优先级从高到低的顺序如下

（续表）

步骤	命令	说明
3	**default-route-advertise** [[**always** | **permit-calculate-other**] | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name* [**match-any**]] * 例如：[Huawei-ospf-10] **default-route-advertise always**	➢ 设置了 **type** 的路由优先于未设置 **type** 的路由，如果都设置了 **type**，值越小越优先 ➢ 设置了 **cost** 的路由优先于未设置 **cost** 的路由，如果都设置了 **cost**，值越小越优先 ➢ 设置了 **tag** 的路由优先于未设置 **tag** 的路由，如果都设置了 **tag**，值越小越优先 【说明】OSPF 路由域中在通告缺省路由前，会比较缺省路由的优先级。如果在其中某 OSPF 设备上同时配置了静态缺省路由和自己通告的缺省路由，要使 OSPF 自己通告的缺省路由加入到当前的路由表中，则必须保证 OSPF 自己通告的缺省路由比所配置的静态缺省路由的优先级高 缺省情况下，在普通 OSPF 区域内的 OSPF 设备不产生缺省路由，可用 **undo default-route-advertise** 命令取消通告缺省路由到普通 OSPF 区域
4	**default-route-advertise summary cost** *cost* 例如：[Huawei-ospf-10] **default-route-advertise summary cost** 10	（可选）在 **ABR** 上发布指定开销的缺省路由的 Type3 LSA，但必须首先使能 VPN，否则缺省路由不能发布。本命令仅用于发布 Type3 缺省路由到普通 OSPF 区域，对于 Stub 区域、Totally Stub 区域、Totally NSSA 区域，缺省路由自动发布。对于 NSSA 区域，则通过 **nssa default-route-advertise** 命令发布缺省路由 缺省情况下，在普通 OSPF 区域内的 OSPF 设备不产生缺省路由，可用 **undo default-route-advertise** 命令取消通告缺省路由到普通 OSPF 区域

12.10.3 配置 OSPF 路由聚合

当 OSPF 网络规模较大时，配置路由聚合可以有效减少路由表中的条目，减小对系统资源的占用。配置路由聚合后，如果被聚合的 IP 地址范围内的某条链路频繁 Up 和 Down，该变化并不会通告到被聚合的 IP 地址范围外的设备（因为被聚合的各子路由最终是以聚合路由对外通告的），可以避免网络中的路由振荡，在一定程度上提高了网络的稳定性。**仅可在运行 OSPF 协议的 ABR 和 ASBR 上配置路由聚合**，具体配置步骤如表 12-19 所示。

说明 在 ABR 或 ASBR 上配置路由聚合后，ABR 和 ASBR 本地的 OSPF 路由表是保持不变的，仍为各网段的明细路由，但是在它们向区域内其他 OSPF 设备通告时，这些连续子网路由将只以一条聚合路由进行通告，这样区域内其他路由器上的 OSPF 路由表中只有这一条聚合路由到达对应聚合网段的路由。直到网络中被聚合的路由**都出现故障**而消失时，该聚合路由才会消失。

在 ASBR 上对引入的路由进行路由聚合后，有以下几种情况。

① 如果本地设备是 ASBR 且处于普通区域中，本地设备将对引入的聚合地址范围内的所有 Type-5 LSA 进行路由聚合。

② 如果本地设备是 ASBR 且处于 NSSA 或者 Totally NSSA 区域中，本地设备对引

入的聚合地址范围内的所有 Type-5 LSA 和 Type-7 LSA 进行路由聚合。

③ 如果本地设备既是 ASBR 又是 ABR 且处于 NSSA 或者 Totally NSSA 区域中，本地设备除对引入的聚合地址范围内的所有 Type-5 LSA 和 Type-7 LSA 进行路由聚合外，还将对由 Type-7 LSA 转化成的 Type-5 LSA 也进行路由聚合。

表 12-19　　OSPF 路由聚合配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图
在 ABR 上配置路由聚合		
3	**area** *area-id* 例如：[Huawei-ospf-10] **area** 1	键入 ABR 所连接的，要配置路由聚合的区域，进入区域视图
4	**abr-summary** *ip-address mask* [[**advertise** | **not-advertise**] | **cost** *cost*]* 例如：[Huawei-ospf-10-area-0.0.0.1]**abr-summary** 36.42.0.0 255.255.0.0	配置 ABR 对区域内路由进行路由聚合（**不能聚合不同区域中的路由**）。ABR 向其他区域发送路由信息时，是以网段为单位生成 Type3 LSA。**当区域中存在连续的网段**（具有相同前缀的路由信息）时，可以通过本命令将这些网段聚合成一个网段，这样，ABR 只需向其他区域发送一条聚合后的 LSA，而不用单独发送，从而减小路由表的规模，提高路由器的性能。命令中的参数和选项说明如下 ● *ip-address mask*：指定聚合路由的 IP 地址和子网掩码。**聚合路由的子网掩码长度肯定要小于所有被聚合路由的子网掩码长度** ● **advertise**：二选一选项，指定同时向被聚合区域和其他区域发布这条聚合路由 ● **not-advertise**：二选一选项，指定不向其他区域发布这条聚合路由，仅向被聚合区域通告这条聚合路由 ● **cost** *cost*：可多选参数，指定聚合路由的开销值，取值范围为 0～16 777 214 的整数。如果不配置此参数，则取所有被聚合的路由中**最大的那个开销值**作为聚合路由的开销 缺省情况下，区域边界路由器不对路由聚合，可用 **undo abr-summary** *ip-address mask* 命令取消在区域边界路由器上进行路由聚合的功能 缺省情况下，区域边界路由器不对路由聚合，可用 **undo abr-summary** *ip-address mask* 命令取消在 ABR 上指定的路由聚合
在 ASBR 上配置路由聚合		
3	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *tag* | **cost** *cost* | **distribute-delay** *interval*]* 例如：[Huawei-ospf-10] **asbr-summary** 10.2.0.0 255.255.0.0 **not-advertise tag** 2 **cost** 100	设置 ASBR 对 OSPF 引入的外部路由进行路由聚合（如果 ASBR 同时是 ABR，则还可进行上面介绍的 ABR 上的路由聚合配置）。命令中的参数和选项说明如下 ● *ip-address mask*：指定聚合路由的 IP 地址和子网掩码。**聚合路由的子网掩码长度肯定要小于所有被聚合路由的子网掩码长度** ● **not-advertise**：可多选选项，设置不向区域内发布该聚合路由，如果不选择此可选项，则向区域内发布该聚合路由 ● **tag** *tag*：可多选参数，指定聚合路由的标记，取值范围为 0～4 294 967 295 的整数。如果不指定此可选参数，缺省值为 1

（续表）

步骤	命令	说明
3	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *tag* | **cost** *cost* | **distribute-delay** *interval*] * 例如：[Huawei-ospf-10] **asbr-summary** 10.2.0.0 255.255.0.0 **not-advertise tag** 2 **cost** 100	• **cost** *cost*：可多选参数，设置聚合路由的开销，取值范围为 0～16 777 214 的整数。如果不配置此可选参数，对于 Type1 类外部路由，取所有被聚合路由中的**最大开销值**作为聚合路由的开销；对于 Type2 类外部路由，则取所有被聚合路由中的**最大开销值再加 1** 作为聚合路由的开销 • **distribute-delay** *interval*：可多选参数，指定延迟发布该聚合路由的时间，取值范围为 1～65 535 的整数秒 缺省情况下，ASBR 不对 OSPF 引入的路由进行路由聚合，可用 **undo asbr-summary** *ip-address mask* 命令取消 ASBR 对 OSPF 引入的路由进行指定的路由聚合

【示例】在 ABR 上将 OSPF 100 的区域 1 中两个网段 36.42.10.0/24、36.42.110.0/24 的路由聚合成一条聚合路由 36.42.0.0/16 向本区域和其他区域同时发布。

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Huawei-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Huawei-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

注意 本示例中，如果区域 1 中还存在其他位于 36.42.0.0/16 网段的子网路由（如 36.42.12.0/24、36.42.15.0/28 等），也将被聚合成该聚合路由。如果不希望这些子网路由被聚合，则不能进行如上的路由聚合配置。

12.10.4 配置 OSPF 对接收和发布的路由进行过滤

OSPF 对接收的路由的过滤**适用于任意 OSPF 路由器**，是通过对接收的路由设置过滤策略，只允许通过过滤策略的路由被添加到本地设备的 OSPF 路由表中，没有通过过滤策略的路由不会被添加进路由表中，自然也不会通过本地设备对外发布。这主要是为了减小本地设备 OSPF 路由表规模，同时抑制一些已有其他路由实现同样效果的路由。

OSPF 对发布的路由的过滤**仅针对在 ASBR 上引入的路由**，通过设置发布策略设备仅允许满足条件的外部路由生成的 Type5 LSA 发布出去，这主要是为了避免路由环路的产生。

OSPF 对接收和发布的路由过滤的配置步骤如表 12-20 所示。

表 12-20 OSPF 对接收和发布的路由过滤的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	启动对应的 OSPF 进程，进入 OSPF 视图

（续表）

步骤	命令	说明
		在任意 OSPF 路由器上配置接收路由的过滤
3	**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**] } **import** 例如：[Huawei-ospf-10] **filter-policy** 2000 **import**	按照过滤策略设置 OSPF 对接收的路由进行过滤。命令中的参数和选项说明如下 ● *acl-number*：多选一参数，指定用于过滤接收路由的基本 ACL 列表号（取值范围为 2 000～2 999 的整数） ● **acl-name** *acl-name*：多选一参数，指定用于过滤接收路由的 ACL 名称（取值范围为 1～32 个字符，**且要以英文字母 a～z 或 A～Z 开始，区分大小写**） ● **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤接收路由的 IP 地址前缀列表名称，取值范围为 1～169 个字符，不支持空格，区分大小写 ● **route-policy** *route-policy-name*：多选一参数，指定用于过滤接收路由的路由策略名称，取值范围为 1～40 个字符 ● **secondary**：可选项，设置优先选择过滤次优路由 【说明】当使用命名型 ACL 过滤接收的路由信息时仅 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则过滤规则有效 缺省情况下，不对 OSPF 接收的路由进行过滤，可用 **undo filter-policy** [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**]] **import** 命令取消 OSPF 对接收的符合指定条件的路由进行过滤
		在 ASBR 上配置发布路由的过滤
3	**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] 例如：[Huawei-ospf-10] **filter-policy** 2000 **export**	在 ASBR 上配置对通过 12.8.1 小节介绍的 **import-route** 命令引入的外部路由进行过滤，只有通过过滤的外部路由才能被发布出去。命令中的参数说明如下 ● *acl-number*：多选一参数，指定用于过滤发布路由的基本 ACL 列表号（取值范围为 2 000～2 999 的整数） ● **acl-name** *acl-name*：多选一参数，指定用于过滤发布路由的 ACL 名称（取值范围为 1～32 个字符，以英文字母 a～z 或 A～Z 开始，区分大小写） ● **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤发布路由的 IP 地址前缀列表名称，取值范围为 1～169 个字符，不支持空格，区分大小写 ● *protocol*：可多选参数，指定要过滤的发布路由信息的协议，目前包括 **direct**、**rip**、**isis**、**bgp**、**ospf**、**unr** 和 **static** ● *process-id*：可多选参数，指定要过滤的发布路由信息的路由进程号，取值范围为 1～65 535 的整数，缺省值是 1。仅当发布的路由协议为 RIP、IS-IS、OSPF 时才可指定 缺省情况下，不对引入的路由在发布时进行过滤，可用 **undo filter-policy** [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*] **export** [*protocol* [*process-id*]] 命令取消对符合条件的引入路由在发布时进行过滤

12.10.5　配置对发送的 LSA 进行过滤

当两台路由器之间存在多条链路时，通过对发送的 LSA 进行过滤可以在某些链路上过滤 LSA 的传送，减少不必要的重传，节省带宽资源。

对发送的 LSA 进行过滤，**可在任意 OSPF 路由器上配置**（除一些特定选项外），具体方法就是在对应的接口视图下使用 **ospf filter-lsa-out** { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }] | **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** {*acl-number* | *acl-name* }] } * }命令进行 LSA 发送过滤策略的配置。命令中的参数和选项说明如下。

① **all**：多选一选项，指定对除 Grace LSA 外的所有 LSA 进行过滤。

② **summary**：可多选选项，对 Type3 LSA 进行过滤，**仅可在 ABR 上配置**。

③ **ase**：可多选选项，对 Type5 LSA 进行过滤，**仅可在普通区域 ABR 上配置**。

④ **nssa**：可多选选项，对 Type7 LSA 进行过滤，**仅可在 NSSA 区域 ABR 上配置**。

⑤ **acl** { *acl-number* | *acl-name* }：可选参数，指定用于过滤 Type3 LSA，或者 Type5 LSA，或者 Type7 LSA 的基本 ACL 列表号（取值范围为 2 000～2 999 的整数）或者 ACL 名称（取值范围为 1～32 个字符，**且需以英文字母 a～z 或 A～Z 开始，区分大小写**）。对于使用命名型 ACL 中的规则进行过滤时，只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则过滤规则有效。

缺省情况下，不对发送的 LSA 进行过滤，可用 **undo ospf filter-lsa-out** 命令取消对 OSPF 接口出方向的 LSA 进行过滤。

【示例】设置 GE1/0/0 接口对出方向除 Grace LSA 外的所有 LSA 进行过滤。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf filter-lsa-out all
```

12.10.6 配置对 ABR Type3 LSA 进行过滤

可在 ABR 上通过对区域内出、入方向的 Type3 LSA 设置过滤条件进一步减少区域间 LSA 的发布和接收。如你不想某个区域中的 Type3 LSA 向另外一个区域发布，或者你不想接收某个区域发来的 Type3 LSA，都可以按照表 12-21 所示的配置进行过滤。

表 12-21　　在 ABR 上过滤 Type3 LSA 的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	在 ABR 上启动对应的 OSPF 进程，进入 OSPF 视图
3	**area** *area-id* 例如：[Huawei-ospf-10] **area** 1	键入要配置 Type3 LSA 过滤的区域，进入区域视图
4	**filter** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** 例如：[Huawei-ospf-10-area-0.0.0.1] **filter** 2000 **export**	（可选）对本区域出方向（也就是发送方向）的 Type3 LSA 进行过滤。命令中的参数说明如下 • *acl-number*：多选一参数，指定用于过滤出方向 Type3 LSA 的基本 ACL 列表号（取值范围为 2 000～2 999 的整数） • **acl-name** *acl-name*：多选一参数，指定用于过滤出方向 Type3 LSA 的 ACL 名称（取值范围为 1～32 个字符，**且要以英文字母 a～z 或 A～Z 开始，区分大小写**）。对于使用命名型 ACL 的规则进行过滤时，只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则过滤规则有效

（续表）

步骤	命令	说明
4	**filter** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** 例如：[Huawei-ospf-10-area-0.0.0.1] **filter** 2000 **export**	• **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤出方向 Type3 LSA 的 IP 地址前缀列表名称，取值范围为 1～169 个字符，不支持空格，区分大小写 • **route-policy** *route-policy-name*：多选一参数，指定用于过滤出方向 Type3 LSA 的路由策略名称，取值范围为 1～40 个字符，不支持空格，区分大小写 缺省情况下，不对区域内出方向的 Type3 LSA 进行过滤，可用 **undo filter** [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export** 命令取消对区域内出方向的 Type3 LSA 进行过滤
5	**filter** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import** 例如：[Huawei-ospf-10-area-0.0.0.1] **filter ip-prefix** my-prefix-list **import**	（可选）对区域内入方向（也就是接收方向）的 Type3 LSA 进行过滤。命令中的参数说明如下 • *acl-number*：多选一参数，指定用于过滤入方向 Type3 LSA 的基本 ACL 列表号（取值范围为 2 000～2 999 的整数） • **acl-name** *acl-name*：多选一参数，指定用于过滤入方向 Type3 LSA 的 ACL 名称（取值范围为 1～32 个字符，**且要以英文字母 a～z 或 A～Z 开始，区分大小写**）。对于使用命名型 ACL 的规则进行过滤时，只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则过滤规则有效 • **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤入方向 Type3 LSA 的 IP 地址前缀列表名称，取值范围为 1～169 个字符，不支持空格，区分大小写 • **route-policy** *route-policy-name*：多选一参数，指定用于过滤入方向 Type3 LSA 的路由策略名称，取值范围为 1～40 个字符，不支持空格，区分大小写 缺省情况下，不对区域内入方向的 Type3 LSA 进行过滤，可用 **undo filter** [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **import** 命令取消对区域内入方向的 Type3 LSA 进行过滤

说明　配置好控制 OSPF 路由信息的各种功能后，可以使用 **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]命令查看 OSPF 接口上的各种过滤配置信息；使用 **display ospf** [*process-id*] **asbr-summary** [*ip-address mask*]命令查看 OSPF ASBR 聚合路由信息。

12.11　调整 OSPF 网络收敛性能

OSPF 路由的收敛性能与路由报文的收敛优先级、各种报文发送和接收定时器参数的配置密切相关。本节主要将具体介绍这些定时器参数的配置方法。

12.11.1　调整 OSPF 网络收敛性能的配置任务

在 OSPF 网络的收敛性能中，可根据应用环境选择其中一项或几项进行配置。

1. 配置路由的收敛优先级

通过配置 OSPF 路由的收敛优先级，允许用户配置特定路由（如对网络收敛性能敏感度较高的业务路由，如 VOD 业务路由、PE 与 PE 之间的端到端路由等）的优先级，使这些路由能够比其他的路由优先进行收敛。

2. 配置 LSA 更新时间间隔

LSA 更新时间间隔是指路由器主动通过 LSU 报文（不是指在收到对方路由器的 LSR 请求报文后而作为应答的 LSU 报文）发布 LSA 更新的时间间隔。通过恰当的设置，可以做到既不会引起网络收敛性能问题，又不会引起网络振荡，也不会消耗过多的其他设备 CPU 资源。

在华为 AR G3 系列路由器中，可以针对不同类型的 LSA 设置不同的更新时间间隔，且可对 Router LSA（Type1 LSA）和 Network LSA（Type2 LSA）采用智能定时器来设置更新时间间隔。在网络相对稳定、对路由收敛时间要求较高的组网环境中，可以指定 LSA 的更新时间间隔为 0 来取消 LSA 的更新时间间隔，使得在网络拓扑或者路由发生变化时可以立即通过 LSA 发布到网络中，从而加快网络中路由的收敛速度。

3. 配置接收 LSA 的时间间隔

前面说的 LSA 更新时间间隔是为了避免过多消耗其他设备 CPU 资源，频繁引起网络振荡而设置的，而此处的接收 LSA 的时间间隔则为了避免过多消耗本地设备的 CPU 资源，频繁引起网络振荡而设置的。

在华为 AR G3 系列路由器中，除了可以手动指定固定的 LSA 接收时间间隔外，还可针对 Router LSA（Type1 LSA）和 Network LSA（Type2 LSA）采用智能定时器来设置接收间隔时间。

4. 配置 SPF 计算的时间间隔

当 OSPF 的链路状态数据库（LSDB）发生改变时，需要重新计算最短路径。如果网络频繁变化，由于需要不断地计算最短路径，会占用大量系统资源，影响设备的效率，同时也会引起网络频繁振荡。在华为 AR G3 系列路由器中，除了可以手动指定固定的 SPF 计算时间间隔外，还可采用智能定时器来设置 SPF 计算间隔时间。

5. 配置接口发送 Hello 报文的时间间隔

Hello 报文是最常用的一种 OSPF 报文，报文内容包括一些定时器的数值、DR、BDR 以及自己已知的邻居，其作用为建立和维护邻接关系，会以设置的 Hello Interval 定时器为时间单位周期性地在使能了 OSPF 的接口上发送。在配置时要注意，OSPF 邻居之间的 Hello 定时器的时间间隔要保持一致，否则不能协商为邻居。

6. 配置相邻邻居失效的时间

邻居失效定时器（Dead Interval）是指在该时间间隔内，若未收到邻居的 Hello 报文，就认为该邻居已失效。通常最少是 Hello Interval 定时器时间值的 4 倍。

7. 配置 Smart-discover

缺省情况下，OSPF 路由器必须等待 Hello 报文发送时间间隔超时后才能再次发送 Hello 报文。这样一来，路由器的邻居状态或者多址网络（广播型或 NBMA）上的 DR、BDR 发生变化时会影响设备间建立邻居的速度。

通过配置 Smart-discover 功能，当网络中邻居状态或者 DR、BDR 发生变化时，设

备不必等到 Hello 报文发送时间间隔超时就可以立刻主动向邻居发送 Hello 报文，从而提高建立邻居的速度，达到网络快速收敛的目的。

12.11.2　调整 OSPF 网络收敛性能的配置步骤

上节介绍的各项配置任务的具体配置步骤如表 12-22 所示（各项配置任务间没有严格的先后次序）。同样，在配置 OSPF 定时器参数之前，需完成以下任务。

① 配置各 OSPF 接口的链路层协议。

② 配置接口的网络层地址，使各相邻节点网络层可达。

③ 配置 OSPF 的基本功能。

表 12-22　　OSPF 网络收敛性能调整的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	在 ABR 上启动对应的 OSPF 进程，进入 OSPF 视图
3	**prefix-priority** { **critical** | **high** | **medium** } **ip-prefix** *ip-prefix-name* 例如：[Huawei-ospf-10] **prefix-priority critical ip-prefix** critical-prefix	（可选）配置 OSPF 路由的收敛优先级。命令中的参数和选项说明如下 ● **critical**：多选一选项，指定本进程中符合参数 *ip-prefix-name* 指定的 OSPF 路由的计算优先级为关键 ● **high**：多选一选项，指定本进程中符合参数 *ip-prefix-name* 指定的 OSPF 路由的计算优先级为高 ● **medium**：多选一选项，指定本进程中符合参数 *ip-prefix-name* 指定的 OSPF 路由的计算优先级为中 ● *ip-prefix-name*：指定用于过滤设置路由优先级的 IP 地址前缀列表的名称，不支持空格，区分大小写，取值范围为 1～169 个字符 【说明】收敛优先级的优先级顺序为：critical>high>medium>low。当一个 LSA 满足多个策略优先级时，最高优先级生效 OSPF 依次按区域内路由、区域间路由、自治系统外部路由顺序进行 LSA 计算，通过本命令可以使 OSPF 按照指定的路由计算优先级分别计算这三类路由。为了加速处理高优先级的 LSA，在泛洪过程中需要按照优先级将相应的 LSA 分别存放在对应的 critical、high、medium 和 low 的队列中 缺省情况下，公网 32 位主机路由的收敛优先级为 **medium**，其他 OSPF 路由的收敛优先级为 **low**，可用 **undo prefix-priority** { **critical** | **high** | **medium** }命令恢复 OSPF 路由为缺省收敛优先级
4	**lsa-originate-interval** { **0** | { **intelligent-timer** *max-interval start-interval hold-interval* | **other-type** *interval* } * } 例如：[Huawei-ospf-10] **lsa-originate-interval** 0	（可选）设置 OSPF LSA 的更新时间间隔。命令中的参数的选项说明如下 ● **0**：二选一选项，指定 LSA 更新的时间间隔为 0，即取消 LSA 的 5 s 的更新时间间隔 ● **intelligent-timer** *max-interval start-interval hold-interval*：可多选参数，指定通过智能定时器分别设置更新 OSPF Router LSA 和 Network LSA 的最长间隔时间（取值范围为 1～10 000 的整数毫秒）、初始间隔时间（取值范围为 0～1 000 的整数毫秒）和基数间隔时间（取值范围为 1～5 000 的整数毫秒）

（续表）

步骤	命令	说明
4	**lsa-originate-interval** { **0** | { **intelligent-timer** *max-interval start-interval hold-interval* | **other-type** *interval* } * } 例如：[Huawei-ospf-10] **lsa-originate-interval** 0	● **other-type** *interval*：可多选参数，指定设置除 OSPF Router LSA 和 Network LSA 外 LSA 的更新间隔时间，取值范围为 0～10 的整数秒，缺省值是 5 【说明】使能智能定时器后 (1) 初次更新 LSA 的间隔时间由 *start-interval* 参数指定 (2) 第 *n*（$n \geqslant 2$）次更新 LSA 的间隔时间为 *hold-interval*×$2^{(n-2)}$ (3) 当 *hold-interval*×$2^{(n-2)}$达到指定的最长间隔时间 *max-interval* 时，OSPF 连续三次更新 LSA 的时间间隔都是最长间隔时间，之后，再次返回步骤 1，按照初始间隔时间 *start-interval* 更新 LSA 缺省情况下，使能智能定时器 intelligent-timer 更新 LSA 的最长间隔时间为 5 000 ms、初始间隔时间为 500 ms、基数间隔时间为 1 000 ms（全是以毫秒为单位），可用 **undo lsa-originate-interval** 命令恢复缺省设置
5	**lsa-arrival-interval** { *interval* | **intelligent-timer** *max-interval start-interval hold-interval* } 例如：[Huawei-ospf-10] **lsa-arrival-interval** 10	（可选）设置 OSPF LSA 接收的间隔时间，命令中的参数说明如下 ● *interval*：二选一参数，指定 LSA 接收的间隔时间，取值范围为 0～10 000 的整数毫秒 ● **intelligent-timer** *max-interval start-interval hold-interval*：二选一参数，指定通过智能定时器分别设置 LSA 接收的最长间隔时间（取值范围为 1～10 000 的整数毫秒）、初始间隔时间（取值范围为 0～1 000 的整数毫秒）和基数间隔时间（取值范围为 1～5 000 的整数毫秒） 【说明】使能智能定时器后 (1) 初次接收 LSA 的间隔时间由 *start-interval* 参数指定 (2) 第 *n*（$n \geqslant 2$）次接收 LSA 的间隔时间为 *hold-interval*×$2^{(n-2)}$ (3) 当 *hold-interval*×$2^{(n-2)}$达到指定的最长间隔时间 *max-interval* 时，OSPF 连续三次接收 LSA 的间隔时间都是最长间隔时间，之后，再次返回步骤 1，按照初始间隔时间 *start-interval* 接收 LSA 缺省情况下，使能智能定时器 intelligent-timer，接收 LSA 的最长间隔时间为 1 000 ms、初始间隔时间为 500 ms、基数间隔时间为 500 ms（全是以毫秒为单位），可用 **undo lsa-arrival-interval** 命令恢复缺省设置
6	**spf-schedule-interval** { *interval1* | **intelligent-timer** *max-interval start-interval hold-interval* | **millisecond** *interval2* } 例如：[Huawei-ospf-10] **spf-schedule-interval** 6	（可选）设置 OSPF 路由计算时间间隔，命令中的参数说明如下。 ● *interval*：多选一参数，以秒为单位指定 OSPF SPF 计算时间间隔，取值范围为 1～10 的整数秒 ● **intelligent-timer** *max-interval start-interval hold-interval*：多选一参数，指定通过智能定时器分别设置 OSPF SPF 计算的最长间隔时间（取值范围为 1～20 000 的整数毫秒）、初始间隔时间（取值范围为 1～1 000 的整数毫秒）和基数间隔时间（取值范围为 1～5 000 的整数毫秒） ● **millisecond** *interval2*：多选一参数，以毫秒为单位指定 OSPF SPF 计算时间间隔，取值范围为 1～10 000 的整数毫秒

（续表）

步骤	命令	说明
6	**spf-schedule-interval** { *interval1* | **intelligent-timer** *max-interval start-interval hold-interval* | **millisecond** *interval2* } 例如：[Huawei-ospf-10] **spf-schedule-interval** 6	【说明】使能智能定时器后 (1) 初次计算 SPF 的间隔时间由 *start-interval* 参数指定 (2) 第 *n*（$n \geqslant 2$）次计算 SPF 的间隔时间为 *hold-interval*$\times 2^{(n-2)}$ (3) 当 *hold-interval*$\times 2^{(n-2)}$达到指定的最长间隔时间 *max-interval* 时，OSPF 连续三次计算 SPF 的时间间隔都是最长间隔时间，之后，再次返回步骤 1，按照初始间隔时间 *start-interval* 计算 SPF 缺省情况下，使能智能定时器 intelligent-timer，SPF 计算的最长间隔时间为 10 000 ms、初始间隔时间为 500 ms、基数间隔时间为 1 000 ms（全是以毫秒为单位），可用 **undo spf-schedule-interval** 命令恢复缺省设置
7	**quit** 例如：[Huawei-ospf-10] **quit**	退出 OSPF 视图，返回系统视图
8	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	进入接口视图
9	**ospf timer hello** *interval* 例如：[Huawei-GigabitEthernet1/0/0]**ospf timer hello** 20	（可选）设置接口发送 Hello 报文的时间间隔，取值范围为 1～65 535 的整数秒。取值越小，网络拓扑改变的速度越快，但相应的路由开销也就越大，**并要确定接口和邻接设备的本参数要保持一致** 缺省情况下，P2P、Broadcast 类型接口发送 Hello 报文的时间间隔的值为 10 s；P2MP、NBMA 类型接口发送 Hello 报文的时间间隔的值为 30 s，可用 **undo ospf timer hello** 命令恢复该时间间隔为缺省值
10	**ospf timer dead** *interval* 例如：[Huawei-GigabitEthernet1/0/0] **ospf timer dead** 60	（可选）设置 OSPF 的邻居失效时间，取值范围为 1～235 926 000 的整数秒，建议配置的失效时间大于 20 s，否则可能会造成邻接关系的中断，**必须大于上一步配置的发送 Hello 报文的时间间隔 hello** *interval*，**且同一网段上的设备的本参数值也必须相同**
11	**ospf smart-discover** 例如：[Huawei-GigabitEthernet1/0/0] **ospf smart-discover**	（可选）在接口上使能 Smart-discover 功能。通过在接口上使能 Smart-discover 功能，设备的邻居状态或者多址网络（广播型或 NBMA）上的 DR、BDR 发生变化时，不必等到 Hello 定时器到时，就立刻主动地向邻居发送 Hello 报文 缺省情况下，接口不使能 Smart-discover 功能，可用 **undo ospf smart-discover** 命令在接口上关闭 Smart-discover 功能

12.12　配置 OSPF 与 BFD 联动

OSPF 通过周期性地向邻居发送 Hello 报文来实现邻居检测，检测到故障所需的时间比较长，超过 1 s。随着科技的发展，语音、视频及其他点播业务应用广泛，而这些业务对于丢包和延时非常敏感，当数据达到吉比特速率级时，较长的检测时间会导致大量数据丢失，无法满足电信级网络高可靠性的需求。

为了解决上述问题，与上一章介绍的静态路由、RIP 路由与 BFD 联动一样，也可以配置指定进程或指定接口的 OSPF 与 BFD 联动特性，以便快速检测链路的状态。其故障检测时间可以达到毫秒级，可提高链路状态变化时 OSPF 的收敛速度。当 BFD 检测到链路故障时，能够将故障通告给路由协议，触发路由协议的快速收敛；当邻居关系为 Down 时，则动态删除 BFD 会话。

说明 目前，BFD 会话不会感知路由切换。如果绑定的对端 IP 地址改变引起路由切换到其他链路上，除非原链路转发不通，否则，BFD 不会重新协商。

1. OSPF 与 BFD 联动的配置流程

配置 OSPF 与 BFD 联动的流程如下（后面两个可选配置任务没有先后次序之分，且可根据实际需要选择配置）。

① 配置全局 BFD 功能。

② 配置全局的 OSPF BFD 特性。

③（可选）阻止接口动态创建 BFD 会话。

仅当要对对应 OSPF 进程下某些接口附上创建 BFD 会话，才需要进行本项配置任务。

④（可选）配置指定接口的 OSPF BFD 特性。

如果希望单独只对某些指定的接口配置与全局配置不一样的 BFD for OSPF 特性，那么当这些接口的链路发生故障时，路由器可以快速地感知，并及时通知 OSPF 重新计算路由，从而提高 OSPF 的收敛速度。当邻居关系为 Down 时，则动态删除 BFD 会话。但在接口上 OSPF 创建 BFD 会话也需要先进行上第一项配置任务，使能全局 BFD 功能。

2. OSPF 与 BFD 联动的配置步骤

以上配置任务的具体配置步骤如表 12-23 所示，在进行这些配置之前，需完成以下任务。

① 配置接口的网络层地址，使各相邻节点网络层可达。

② 配置 OSPF 的基本功能。

表 12-23 OSPF 与 BFD 联动的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
配置全局 BFD 功能	2	**bfd** 例如：[Huawei] **bfd**	配置全局 BFD 功能并进入全局 BFD 视图
配置全局的 OSPF BFD 特性	3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
	4	**ospf** [*process-id*] 例如：[Huawei] **ospf** 10	进入 OSPF 视图
	5	**bfd all-interfaces enable** 例如：[Huawei-ospf-10] **bfd all-interfaces enable**	打开 OSPF BFD 特性的开关，建立 BFD 会话。这样，当配置了全局 BFD 特性，且邻居状态达到 Full 时，OSPF 为该进程下所有具有邻接关系的邻居建立 BFD 会话

（续表）

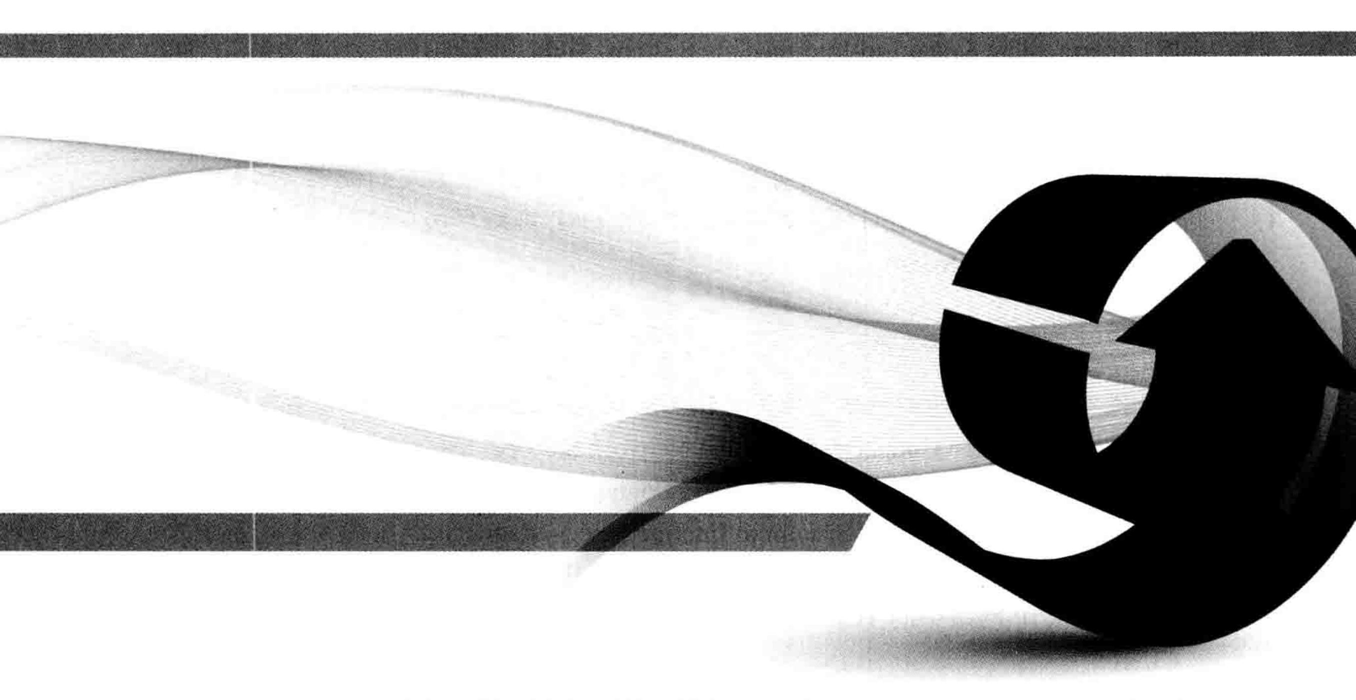
配置任务	步骤	命令	说明
配置全局的 OSPF BFD 特性	6	**bfd all-interfaces** { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier***multiplier-value* | **frr-binding** } * 例如：[Huawei-ospf-10] **bfd all-interfaces min-tx-interval** 400	（可选）指定需要建立 BFD 会话的各个参数值。命令中的参数说明如下 ● **min-rx-interval** *receive-interval*：可多选参数，指定期望从对端接收 BFD 报文的最小接收间隔，取值范围为 10～2 000 的整数毫秒，缺省值是 1 000 ms ● **min-tx-interval** *transmit-interval*：可多选参数，指定向对端发送 BFD 报文的最小发送间隔，取值范围为 10～2 000 的整数毫秒，缺省值是 1 000 ms ● **detect-multiplier***multiplier-value*：可多选参数，指定本地检测倍数，取值范围为 3～50 的整数，缺省值是 3 ● **frr-binding**：可多选选项，将 BFD 会话状态与接口的链路状态进行绑定。当 BFD 会话状态变为 Down 时，接口的物理层链路状态也会变为 Down，从而触发流量切换到备份路径。**但 AR150/150-S/160/200/200-S 系列不支持该选项** 【说明】具体参数如何配置取决于网路状况以及对网络可靠性的要求，对于网络可靠性要求较高链路，可以减小 BFD 报文实际发送时间间隔；对于网络可靠性要求较低的链路，可以增大 BFD 报文实际发送时间间隔。但使能 BFD 特性后，OSPF 只和状态达到 Full 的邻居建立起 BFD 会话 ● 本地 BFD 报文实际发送时间间隔＝MAX {本地配置的发送时间间隔 *transmit-interval*，对端配置的接收时间间隔 *receive-interval* } ● 本地 BFD 报文实际接收时间间隔＝MAX {对端配置的发送时间间隔 *transmit-interval*，本地配置的接收时间间隔 *receive-interval* } ● 本地 BFD 报文实际检测时间＝本地实际接收时间间隔×对端配置的 BFD 检测倍数 *multiplier-value* 缺省情况下，在 OSPF 进程下不使能 BFD 特性，可用 **undo bfd all-interfaces** { **min-rx-interval** | **min-tx-interval** | **detect-multiplier** | **frr-binding** } * 命令恢复对应 BFD 会话参数为缺省值
	7	**quit** 例如：[Huawei-ospf-10] **quit**	退出 OSPF 视图，返回系统视图
（可选）阻止接口动态创建 BFD 会话	8	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要阻止动态 BFD 会话的接口，进入接口视图
	9	**ospf bfd block** 例如：[Huawei-GigabitEthernet1/0/0] **ospf bfd block**	（可选）阻止以上接口动态创建 BFD 会话。因为在执行完第 3 步的 **bfd all-interfaces enable** 命令后，该进程下所有使能 OSPF 且邻居状态为 Full 的邻居都将创建 BFD 会话。如果不希望某些接口使能 BFD 特性，则需要在这些接口上配置本命令阻止动态创建 BFD 会话 缺省情况下，不阻塞接口动态创建 BFD 特性，可用 **undo ospf bfd block** 或者 **ospf bfd enable** 命令取消该阻塞特性

（续表）

配置任务	步骤	命令	说明
（可选）阻止接口动态创建BFD会话	10	**quit** 例如：[Huawei-ospf-10] **quit**	退出接口视图，返回系统视图
（可选）配置指定接口的OSPF BFD特性	11	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 2/0/0	键入要使能BFD特性的OSPF接口，进入接口视图
	12	**ospf bfd enable** 例如：[Huawei-GigabitEthernet2/0/0] **ospf bfd enable**	打开接口BFD特性的开关，建立BFD会话
	13	**ospf bfd** { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } * 例如：[Huawei-GigabitEthernet2/0/0] **ospf bfd min-rx-interval** 400 **detect-multiplier** 4	（可选）在使能了OSPF的接口下配置BFD特性和BFD会话的参数值。具体参数和其他说明参见本表第4步，只不过这里是针对特定接口配置的 【说明】接口下的BFD会话参数配置优先级高于第4步在OSPF进程下进行的BFD会话参数配置。即如果在OSPF进程和具体接口下都进行了BFD会话参数配置，则该接口将以本步配置为准 缺省情况下，OSPF接口下不使能BFD特性，可用 **undo ospf bfd** { **min-rx-interval** | **min-tx-interval** | **detect-multiplier** | **frr-binding** } *命令取消对应接口下的BFD特性，恢复BFD会话参数为缺省值



第13章 IS-IS路由配置与管理



IS-IS（中间系统到中间系统）协议与上章介绍的OSPF（开放最短路径优先）协议有许多类似之处，如都是链路状态的IGP路由协议，采用的都是SPF路由算法，都划分了区域，都可以在一台路由器上运行多个路由进程，都主要应用于大型网络、甚至互联网等。

当然，它们之间还存在许多不同之处，如在OSPF路由协议中，一个路由器可以同时位于多个区域中，但在IS-IS中，一个路由器却只能位于一个区域中，而且OSPF中规定区域0是骨干区域，而在IS-IS中骨干区域是不固定的，它是与Level-2路由器一起组成的区域；OSPF中的指定路由器（DR）一经配置就是固定的，而IS-IS中的指定路由器（DIS）却要经过选举，随时可能改变，并且没有备份指定路由器等。

本章首先将介绍IS-IS路由协议各方面的基础知识，如区域划分、路由器类型、路由器邻接、LSP PDU的格式以及IS-IS邻居关系建立、LSP报文交互、IS-IS报文验证、IS-IS路由渗透和网络收敛原理，然后介绍了IS-IS基本功能、IS-IS路由聚合、IS-IS路由信息交互控制、IS-IS路由选路、IS-IS网络收敛性能调整、IS-IS安全验证和IS-IS与BFD联动等配置与管理方法。同时，各主要部分还将有大量配置示例介绍，以便读者加深对基础原理和配置方法的理解。

13.1 IS-IS 基础

IS-IS（Intermediate System-to-Intermediate System，中间系统到中间系统）最初是 ISO（国际标准化组织）为它定义的 OSI（Open System Interconnection，开放系统互联）网络中的 CLNP（ConnectionLess Network Protocol，无连接网络协议）设计的一种动态路由协议。随着 TCP/IP 的流行，为了提供对 IP 路由的支持，IETF 在 RFC1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 网络环境中，称为集成 IS-IS（Integrated IS-IS 或 Dual IS-IS）。

13.1.1 OSI 网络基础

在 OSI 网络中定义了两类网络层服务：CLNS（Connectionless Network Service，无连接网络服务）和 CONS（Connection-oriented Network Service，面向连接的网络服务）。其中，提供 CLNS 服务的协议主要包括 CLNP（Connectionless Network Protocol，无连接网络协议）、IS-IS 和 ES-IS（End System to Intermediate System，终端系统到中间系统），它们分别起着不同的作用。CLNS 类似于 TCP/IP 中的 IP 协议簇，都是无连接服务；而 CONS 类似于 TCP/IP 网络中的 TCP，都是面向连接的服务。

1. CLNP

CLNP 是 OSI 网络的网络层数据报协议，提供了与 TC/IP 网络中 IP 类似的功能，因此 CLNP 又称之为 ISO-IP。与 IP 一样，CLNP 也是一个无连接的网络层协议，提供无连接的网络层服务。但是，IP 是 TCP/IP 协议栈中唯一的网络层协议，来自高层的协议和数据绝大多数需要封装在 IP 协议报文中，然后再传输到数据链路层，重新封装在帧中进行传输。而在 OSI 网络环境中，前面说的 CLNP、IS-IS、ES-IS 都是独立的网络层协议，都直接被封装到数据链路层的帧中进行传输。CLNP 使用 NSAP（网络服务访问协议）地址来识别网络设备。

2. IS-IS

IS-IS 协议最早是由 DEC 公司于 20 世纪 80 年代后期开发的，并在 ISO/IEC 10589 中以标准形式发布，是一种动态路由协议。IS-IS 最初仅用于在使用 CLNP 的 OSI 网络中实现各路由器间路由信息交换。随着 TCP/IP 的流行，为了提供对 IP 路由的支持，IETF 在 RFC1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 网络环境中，也就是前面所说的“集成 IS-IS”（Integrated IS-IS 或 Dual IS-IS）。再后来的 IETF 标准扩展又定义了 IS-IS 对 IPv6 网络的支持。目前的 IS-IS 版本为 ISO/IEC 10589:2002，可以全面支持 OSI 和 TCP/IP 网络环境。

说明 从以上可以看出，IS-IS 是一个能够同时处理多个网络层协议（例如 IP 和 CLNP）的路由选择协议。而上一章介绍的同属于链路状态路由协议的 OSPF 协议只支持 IP 一种网络层协议，即 OSPF 仅支持 IP 路由，专为 TCP/IP 网络设计。

3. ES-IS

ES-IS 也是由 ISO 开发，用来允许终端系统（如 PC 机）和中间系统（指路由器）进

行路由信息的交换（也就是通常所说的 PC 主机与路由器之间的路由），以推动 OSI 网络环境下网络层的路由选择和中继功能的操作。ES-IS 在 CLNP 网络中就像 IP 网络中的 ARP、ICMP 一样，为用户主机与路由器间提供路由信息交换功能。

13.1.2　IS-IS 基本术语

要正确理解 IS-IS 路由协议工作原理，首先要理解以下基本专业术语。

1. IS（Intermediate System，中间系统）

IS 是指运行 IS-IS 协议的路由设备。它是 IS-IS 协议中生成路由和传播路由信息的基本单元。在本章后面讲的 IS 和路由器具有相同的含义。

2. ES（End System，终端系统）

ES 相当于通常所说的主机系统。ES 不参与 IS-IS 路由协议的处理，在 OSI 网络环境中使用专门的 ES-IS 协议定义 ES 与 IS 间的路由通信。

3. RD（Routing Domain，路由域）

RD 是指由多个使用 IS-IS 协议的路由器所组成的范围。

4. Area（区域）

Area 是 IS-IS 路由域的细分单元。IS-IS 与 OSPF 一样，允许将整个路由域分为多个区域，且总体上也分为普通区域和骨干区域两类，但 IS-IS 的普通区域必须与骨干区域直接连接（没有 OSPF 中的“虚连接”），普通区域之间不能直接连接。Area 又可根据网络中路由器的类型划分为 Level-1 区域（全由 Level-1 路由器组成）和 Level2 区域（由 Level-2 和 Level-1-2 路由器组成），有关路由器类型将在下节具体介绍。

5. Sys ID（System ID，系统 ID）

在 IS-IS 协议中使用 Sys ID 唯一标识一台路由器，必须保证在整个 IS-IS 路由域中每台路由器的系统 ID 都是唯一的，与 OSPF 中的路由器 ID（Router ID）一样。

6. LSP（Link-State Packet，链路状态报文）

ISP 是 IS-IS 网络中的设备用来通过泛洪方式向所有邻居通告自己的链路状态信息的报文，类似于 OSPF 中的 LSA（链路状态通告）。网络中每台路由器都会产生带有自己系统 ID 标识的 LSP 报文，可以通过发送 LSP 不断更新自己的链路状态信息。

7. LSDB（Link State DataBase，链路状态数据库）

路由器的每个区域都有一个专门存放该区域所接收的所有 LSP 报文的数据库，这就是 LSDB。通过 LSP 的泛洪，最终使整个区域内的所有路由器拥有相同的 LSDB。在每一个 IS 中都至少有一个 LSDB，那就是 Level-2 LSDB。IS-IS 路由器利用各个区域的 LSDB，通过 SPF 算法（与 OSPF 协议使用的算法一样）计算生成自己的 IS-IS 路由表。

8. DIS（Designated IS，指定 IS）

在 IS-IS 广播网络类型中需要选举一个指定 IS（DIS），以便周期性地向区域内其他路由器进行区域 LSDB 数据库的泛洪（**区域内的非 DIS 仅与 DIS 之间进行 LSDB 交互，非 DIS 之间不能直接进行 LSDB 交互**），使整个区域中各路由器的 LSDB 同步。DIS 的功能类似于 OSPF 中的 DR（指定路由器），但是在 OSPF 中有备份 BDR（备份指定路由器）的概念，IS-IS 中没有备份的 DIS 概念。

13.1.3 IS-IS 路由器类型

OSPF 协议根据路由器所处的网络位置以及作用不同，把网络中的所有路由器划分为区域内部路由器、骨干路由器、区域边界路由器、自治系统边界路由器类似。IS-IS 协议也根据各路由器所处的网络位置不同，或者作用不同分成了三类：Level-1（简称 L1）、Level-2（简称 L2）和 Level-1-2（简称 L1/2）。所有 IS-IS 路由器缺省都是 L1/2 类型的。下面分别介绍这三种 IS-IS 路由器及各自可以有的邻接关系。

说明 IS-IS 的这些路由器类型也与所处的区域类型有关。IS-IS 中的区域与 OSPF 中的区域也是类似的，分为普通区域和骨干区域两大类，但 IS-IS 中的骨干区域不固定区域 ID（可任意），且可以有多个区域 ID 不同的骨干区域，这点与 OSPF 是完全不同的（OSPF 中的骨干区域 ID 总为 0，且如果有多个分离的骨干区域，它们的 ID 都是 0）。有关 IS-IS 中的区域将在 13.1.5 小节中具体介绍。

1. L1 路由器

L1 路由器是一个 IS-IS **普通区域内部**的路由器，类似于 OSPF 网络中的普通区域内部路由器（IR），**只能在非骨干区域中存在**。而且 L1 路由器只能与属于同一区域的 L1 和 L1/2 路由器建立 L1 邻接关系（**不能与 L2 路由器建立邻接关系**），交换路由信息，并维护和管理本区域内部的一个 L1 LSDB。

L1 路由器的邻居都在同一个区域中，其 LSDB 包含本区域的路由信息以及到达同一区域中最近 L1/2 路由器（相当于 OSPF 中的 ABR，下面将下介绍）的缺省路由，但到区域外的数据需由最近的 L1/2 路由器进行转发。也就是说，L1 路由器只能转发区域内的报文，或者将到达其他区域的报文转发到距离它最近，且在同一区域的 L1/2 路由器。

2. L2 路由器

L2 路由器是**骨干区域**中的路由器，主要用于通过与普通区域中的 L1/2 路由器（下面将介绍）连接，连接骨干区域和非骨干区域，类似于 OSPF 网络中的 BR（骨干路由器），并负责在不同区域间的通信。

L2 路由器只能与其他 L2 路由器共处一个区域，L2 路由器可与本区域中的其他 L2 路由器，以及其他区域中的 L1/2 路由器建立 L2 邻接关系，交换路由信息，维护一个 L2 的 LSDB。网络中的所有 L2 路由器和所有 L1/2 路由器连接在一起共同构成 IS-IS 网络的骨干网（**注意，不是骨干区域**），也称 L2 区域。IS-IS 中的 L2 区域不是一个特定的区域，是由连接网络中各个区域的一部分路由器组成的，**但必须物理是连续**。而 IS-IS 网络中所有 L1 路由器与 L1/2 路由器连接所形成的区域统称为 L1 区域。**L1 区域是分散的，不是连续的**。

在图 13-1 所示的网络中，一般都认为用箭头标注的那台 IS-IS 路由器应该是 L1 路由器，因为它是在一个普通区域之内。但事实上是错误的，因为这样一来，整个网络中由 L2 路由器和 L1/2 路由器形成的骨干网（**粗线部分**）在物理上就是断开的，不连续，最终导致的结果就是不同区域间的 L2 路由无法传递。所以图中用箭头标注的这台路由器必须也是 L1/2 类型的，不能是 L2 类型的，因为 Area2 是非骨干区域。

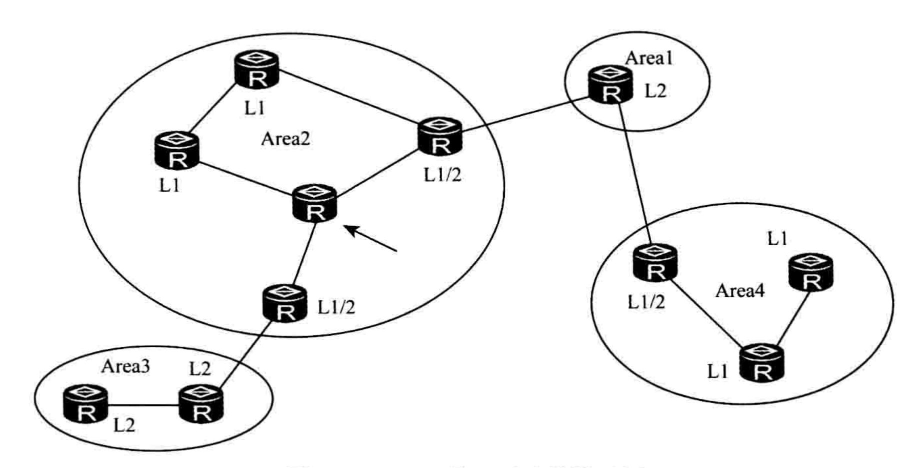


图 13-1　IS-IS 骨干网连续性示例

3. L1/2 路由器

L1/2 路由器类似于 OSPF 网络中的 ABR（区域边界路由器），用于区域间的连接，缺省所有 IS-IS 路由器都是 L1/2 类型的。L1/2 路由器既可以与同一普通区域的 L1 路由器以及其他 L1/2 路由器建立 L1 邻接关系，也可以与骨干区域 L2 路由器建立 L2 邻接关系。L1 路由器必须通过 L1/2 路由器才能与其他区域通信。L1/2 路由器必须维护以下两个 LSDB：L1 LSDB 用于区域内路由，L2 LSDB 用于区域间路由。但要注意的是，**L1/2 路由器不一定要位于区域边界，在区域内部也有可能存在 L1/2 路由器**，图 13-1 中箭头指示的那台路由器就不是位于区域边界。

13.1.4　OSI 网络/IS-IS 路由类型

通过前面的介绍我们已经知道，IS-IS 最初是为 OSI 网络而开发的网络层路由协议，所以它的路由选择功能就与 TCP/IP 网络中的路由功能在实现上有些不一样。

在整个 OSI 网络中，包括了 4 个路由级别（或称 4 种路由类型）：L0（Level-0）、L1（Level-1）、L2（Level-2）和 L3（Level-3）。IS-IS 所能提供的路由仅包括 L1、L2 这两个级别。

1. L0 路由

L0 路由是 OSI 网络中 ES 与 IS 之间的路由（**不属于 IS-IS 协议所提供的路由功能**），使用 ES-IS 协议进行路由信息交换。在 ES-IS 协议中，ES 通过侦听 IS 发送的 IIH 报文（IS 到 IS 的 Hello 报文）来获知 IS 的存在。当 ES 要向其他 ES 发送 ESH 报文（ES 到 ES 的 Hello 报文）时将同时把报文发送到 IS。同样，IS 也会侦听 ES 发送的 ESH 报文以获知 ES 的存在，当有数据要发送到某个 ES 时，会根据所获取的 ESH 信息进行发送。这个过程就称为 L0 路由选择过程。

2. L1 路由

L1 路由是 OSI 或者 TCP/IP 网络中在同一普通区域内各 IS 之间的路由，即普通区域内路由，**是 IS-IS 协议提供的路由功能**。同一个普通区域中的 IS 之间通过交换路由信息后，便得知了本区域内的所有路径。当 IS 收到一个到目标地址是本区域内地址的报文后，通过查看包的目的地址即可将报文发往正确的链路或目的节点。能提供 L1 路由的 IS-IS

路由器类型有 L1 路由器和 L1/2 路由器。

【经验之谈】尽管同一普通区域内部 IS 间路由仅需要 L1 路由即可，但是并不能就此推断，在同一普通区域中的 IS 都只能是 L1 路由器，也可以是同时支持 L1 路由和 L2 路由的 L1/2 路由器，只是说 L1 路由是仅用于区域内部的路由。

3. L2 路由

L2 路由是 OSI 或者 TCP/IP 网络中不同区域间各 IS 之间的路由，即区域间路由，**也是 IS-IS 协议提供的路由功能**。当一个 IS 收到一个目的地址不是本区域 CLNP 地址的报文时，便将其转发到正确的目的地或者将报文转发到其他区域，以便由其他区域中的 IS 转发到正确的目的地。能提供 L2 路由的 IS-IS 路由器类型有 L2 路由器和 L1/2 路由器。

【经验之谈】尽管 L2 路由是用于 IS-IS 区域间的路由，但是 L2 路由也可能需要在区域内部传递，如骨干区域内部，甚至在普通区域内部的多个 L1/2 路由器之间。为了既能提供普通区域内部的 L1 路由，又能传递不同区域间的 L2 路由，所以在普通区域内部（不一定位于区域边界）的路由器也可能是 L1/2 类型，具体参见上节的图 13-1。

4. L3 路由

L3 路由是 OSI 网络中不同 IS-IS 路由域间的路由，**不属于 IS-IS 提供的路由功能。**L3 路由类似于 TCP/IP 网络中的 BGP（Border Gateway Protocol，边界网关协议），其目的是在不同的路由域或自治系统（AS）间交换路由信息，并将去往其他 AS 的包转发到正确的 AS，以便到达最终目的地。这些 AS 之间可能拥有不同的路由拓扑，所以不能直接进行路由信息的交换。通常 L3 路由是由 IRDP（Inter-Domain Routing Protocol，域间路由选择协议）来完成的。

从以上分析可看出，IS-IS 所能完成的路由功能包括上面所介绍的 L1 和 L2 路由功能（同时提供 L1 和 L2 的路由称之为 L1/2 路由），这仅是整个 OSI 网络中路由选择功能的一部分。

13.1.5 IS-IS 区域与 OSPF 区域的比较

IS-IS 网络与 OSPF 网络一样也可以划分多个区域，但是 IS-IS 是工作在数据链路层的，其报文直接以帧格式封装；而 OSPF 是工作在应用层的，其报文需要由网络 IP 报文格式进行封装。所以它们两者划分区域的方法是不一样的，但在 IS-IS 与 OSPF 区域之间仍有诸多不同之处。

1. IS-IS 可以有多个骨干区域

OSPF 的设计基于骨干区域，而且只有一个骨干区域（区域号固定为 0），所有的非骨干区域（通过 ABR）必须直接与骨干相连（非骨干区域与骨干区域之间没有直接物理连接的话，则要通过虚链路连接）。而 **IS-IS 中可以有多个骨干区域，且骨干区域 ID 不固定**，即任意，但它与 OSPF 一样要求所有的非骨干区域（通过 L1/2 路由器）必须直接与骨干相连，普通区域之间不能直接连接。IS-IS 中的骨干区域全由 L2 路由器构成，在骨干区域内部必须与其他 L2 路由器直连，在与普通区域之间，必须与 L1/2 路由器相连，不能与 L1 路由器相连。

图 13-2 所示为一个运行 IS-IS 协议的典型网络结构。在这种拓扑结构中，Area 1 是骨干区域（可以是其他区域号），该区域中的所有路由器均是 L2 路由器。另外 4 个区域

为非骨干区域，它们都通过 L1/2 路由器与 L2 路由器相连。

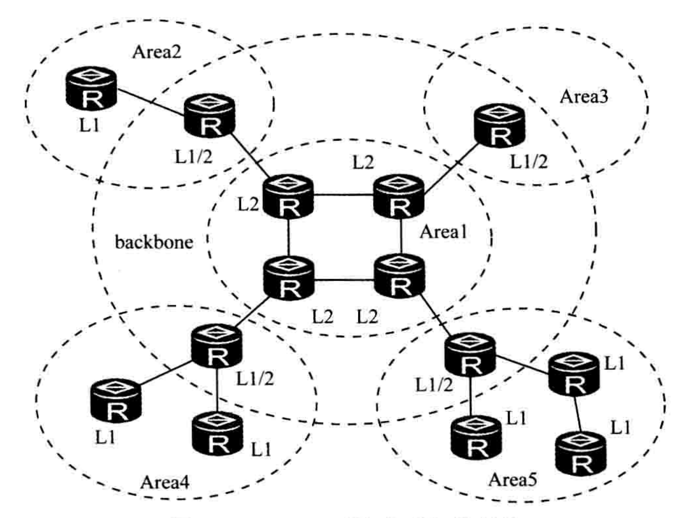


图 13-2　IS-IS 网络典型拓扑结构

图 13-3 所示为 IS-IS 网络的另外一种拓扑结构图，其中有两个骨干区域（Area 1 和 Area 3）。非骨干区域中的 L1/2 路由器同时与两个骨干区域的 L2 路由器连接，同时两个骨干区域之间也彼此连接（可以把它们看成一个大的虚拟骨干区域），这两部分共同构成了一个 IS-IS 骨干网（**也称 L2 区域**）。即 IS-IS 骨干网是由所有的 L2 路由器和各区域边界的 L1/2 路由器构成，它们可以属于不同的区域，**但必须是物理连续**，即中间不能为 L1 路由器。这部分可参见 13.1.3 小节的图 13-1。

2. 区域边界不同

OSPF 的区域边界在设备接口上，OSPF 的每条链路的两端接口都必须属于同一个区域，如图 13-4 所示。这样一来，在 OSPF 中，一台路由器的不同接口可以属于多个不同区域。而在 IS-IS 的区域边界在链路上，即**同一链路的两端接口分属不同区域**（参见图 13-3 和图 13-4），不同区域的边界仅体现在不同区域间连接的链路上，而不是像 OSPF 那样体现在不同路由器接口上。这样一来，**一台 IS-IS 路由器的各个接口都必须同属一个区域。**

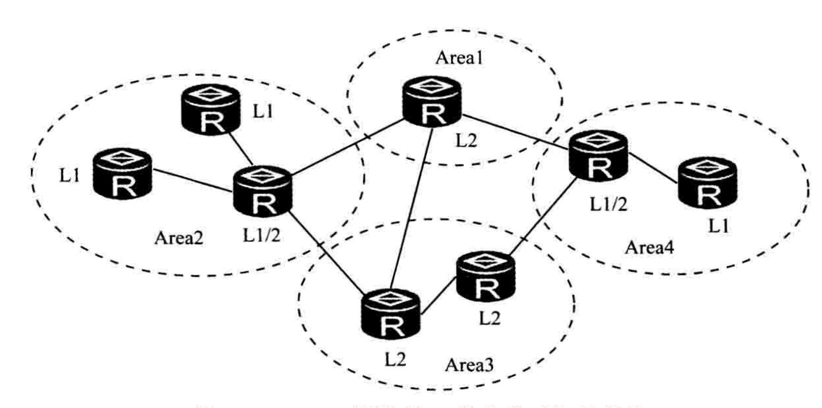


图 13-3　IS-IS 网络的一种非典型拓扑结构

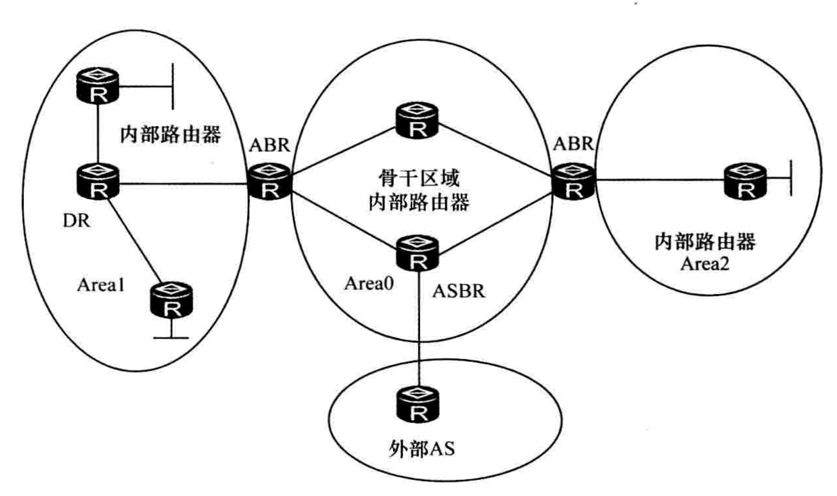


图 13-4 OSPF 中的区域边界示例

3. 不同区域间路由器的邻接关系不同

OSPF 协议使用路由器接口来划分区域，一台路由器可能同时属于多个区域，并可以与多个区域的路由器形成邻接关系。而 IS-IS 协议规定路由器整体属于某个特定的区域，L1 路由器只能建立 L1 级邻接关系；L2 路由器只能建立 L2 级邻接关系；L1/2 既可以与 L1 路由器建立 L1 级邻接关系，又可以与 L2 或者其他 L1/2 路由器建立 L2 级邻接关系。即在 IS-IS 路由协议中，只有同一层次的相邻路由器才可能成为邻接体。具体邻接关系的建立规则如下。

① 同一区域的 L1 路由器间可以建立 L1 级邻接，不同区域的 L1 路由器间不可能建立任何邻接关系。

② 同一区域的 L1 路由器和 L1/2 路由器间可以建立 L1 级邻接，但不能与不同区域的 L1/2 路由器和 L2 路由器间建立任何邻接关系。

③ 同一区域的 L1/2 路由器间可以建立 L1 和 L2 级邻接关系，但不同区域的 L1/2 路由器间可以建立 L2 级邻接关系。

④ 同一骨干区域的 L2 路由器间可以建立 L2 级邻接关系。

⑤ 骨干区域的 L2 路由器与普通区域中的 L1/2 路由器间可以建立 L2 级邻接关系。

4. SPF 路由算法的使用不同

在 IS-IS 中，普通区域内的 L1 路由、区域间和骨干区域内部的 L2 路由都是采用 SPF 算法进行计算的，分别生成各自的 SPT（Shortest Path Tree，最短路径树）；而在 OSPF 中只有在同一个区域内才使用 SPF 算法，区域之间的路由需要通过骨干区域来转发。

13.1.6 IS-IS 的两种地址格式

在 IS-IS 协议中有两种地址：一种是用来标识网络层服务的 NSAP（Network Service Access Point，网络服务访问点）地址，另一种是用来标识设备的 NET（Network Entity Titile，网络实体名称）地址。下面分别予以介绍。

1. NSAP 地址格式

NSAP 地址仅适用于 OSI 网络，用来标识 CLNS 网络层地址，每个通信进程（不是

每个接口）对应一个 NSAP 地址，类似于 TCP/IP 网络中的 Socket 套接字服务。

NSAP 地址由两个主要部分组成，IDP（Inter-Domain Portion，域间部分）和 DSP（Domain Service Portion，域服务部分），如图 13-5 所示。这与 IP 地址中由网络 ID 和主机 ID 两部分组成类似：其中的 IDP 部分相当于 TCP/IP 网络 IP 地址中的主网络 ID 部分，而 DSP 部分则相当于 TCP/IP 网络 IP 地址中的子网 ID、主机 ID 和端口号总和。

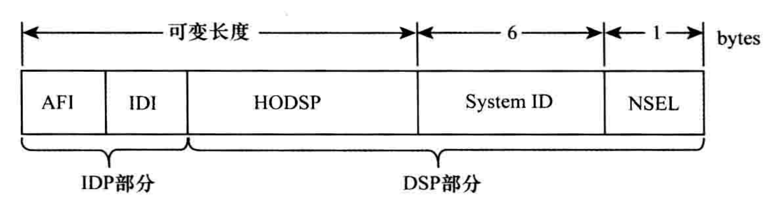


图 13-5　IS-IS NSAP 地址格式

IDP 由以下这两个子部分组成。

① AFI（Authority and format ID，颁发机构与格式 ID）：用来标识 NSAP 地址格式和对应地址的分配机构，占 1 个字节。AFI 等于 49 的地址是私有地址，就像 IP 地址中的局域网地址一样，而 AFI 等于 39 或 47 的地址属于 ISO 注册地址，相当于 IP 地址的公网地址。

② IDI（Inter-Domain ID，域间 ID）：用来标识、区分 AFI 字段下不同的 IS-IS 路由域，最长可达 10 个字节。

DSP 由以下三个子部分组成。

① HODSP（High Order DSP，DSP 高位）：用来在一个 IS-IS 路由域中分割多个区域，相当于 IP 地址中的子网 ID 部分。

② SID（System ID，系统 ID）：占 6 个字节，用来区分主机，通常以 MAC 地址进行标识，类似于 OSPF 协议中的路由器 ID，相当于 IP 地址中的主机 ID 部分。LSP 的识别就是依据路由器 NSAP 地址中的系统 ID。当 IS 工作在 L1 时，则在所有同区域中的 L1 路由器的系统 ID 必须唯一；当 IS 工作在 L2 时，则在同一个路由域中所有路由器的系统 ID 必须唯一。

③ NSEL（Network-Selector，网络选择器）：占 1 个字节，用来指示选定的服务，相当于 TCP 协议中的端口号。在 IS-IS 路由选择过程中没有使用 NSEL，所以 NSEL 始终保持为 00。

从以上可以看出，NSAP 地址中包含了很多不同的字段，看起来有些复杂。但实际上可以将 NSAP 地址进行简化，各种字段可以归类为 3 个部分：区域地址（Area address）、System ID 和 NSEL，如图 13-6 所示。其中“Area Address”（区域地址）包括了图 13-5 中的 AFI、IDI 和 HODSP 这三个字段，长度可变，在 1～13 个字节之间。System ID 和 NSEL 这两部分与图 13-5 中的对应字段一样，参见前面介绍即可。

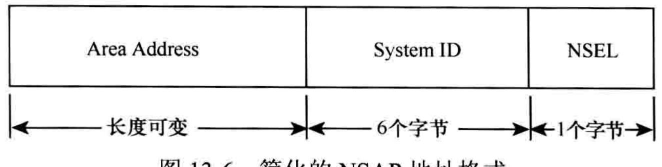


图 13-6　简化的 NSAP 地址格式

由于一般情况下 1 字节（2 个十六进制数字）的长度足够定义 Area Address，所以在大多数的 IS-IS 实现中 NSAP 地址最小长度为 8 字节。对于 IP 应用程序而言，在 NSAP 地址中，1 字节定义 AFI（也是 2 个数字），最少 2 字节定义实际的区域信息（IDI），6 字节定义 System ID，1 字节定义 NSEL，所以此种情况下的 NSAP 地址最少为 10 字节。

2. NET 地址格式

在 IP 网络的 IS-IS 协议中，IS-IS 路由器是以 NET（Network Entity Title，网络实体名称）地址进行标识的。NET 也是一种 NSAP 地址，只是没有使用 OSI 网络中 NSAP 地址的 NSEL 部分，所以 NSEL 始终保持为 00。

路由器在发送的 LSP 报文中用 NET 来标识自己，这类似于 OSPF 发送的 LSA 中的路由器 ID（Router ID）。通常情况下，一台路由器只需配置一个 NET 即可，当区域需要重新划分时，由于最多可配置 3 个区域，所以 NET 最多也只能配置 3 个。

NET 地址的整个长度范围与 NSAP 一样，也是 8～20 个字节，分成三个部分（参见图 13-6）。

① 区域地址（Area Address)：是整个地址的最高字节序列，长度范围为 1～13 个字节，相当于 OSPF 网络中的“区域 ID”。一个 IS-IS 路由进程示例可以配置多个区域地址，此时所有区域地址都具有相同含义，主要用于区域合并或者区域划分。可以简单地配置成 0000.0000.0001、0000.0000.0002 和 0000.0000.0003 格式（各数字均为十六进制）。

② 系统 ID（System ID)：它是继“区域地址”字段后的 6 个字节，并且是以数字开始的。当路由器为 L1 IS 时，则该 IS 的系统 ID 必须在同一区域中的所有 L1 IS 中唯一；当路由器为 L2 IS 时，则该 IS 的系统 ID 必须在整个 IS-IS 路由域中唯一。

可以把路由器环路接口 IP 地址转换为系统 ID，只需要把每个字节都用 3 个数字来表示，然后再转换成三段（原来 IP 地址是四段）即可。如先将 192.31.231.16 转换成 192.031.231.016，再转换成三段得到 1920.3123.1016 即可，这样就可用作系统 ID 了。

③ NSEL（网络选择器)：在“系统 ID”字段之后的 1 个字节，其值总为“00”。

如果一个 NSAP 地址为 49.0001.aaaa.bbbb.cccc.00，根据图 13-6 可以很快得出，代表的“区域地址”为 49.0001（因 AFI=49，所以它是一个私有地址），系统 ID 为 aaaa.bbbb.cccc，NESL 为 00。如果另一个 NSAP 地址为 39.0f01.0002.0000.0c00.1111.00，则可以得出“区域地址”为 39.0f01.0002（因 AFI=39，所以它是一个公有地址），系统 ID 为 0000.0c00.1111，NSEL 为 00。

13.2 IS-IS PDU 报文格式

IS-IS 路由协议和其他路由协议不同，它直接运行在数据链路层之上，对等路由器间通过 PDU（协议数据单元）来传递链路状态信息，完成链路状态 PDU 数据库（LSPDB）的同步。

13.2.1 IS-IS 主要 PDU 类型

IS-IS 网络中使用的 PDU 类型主要有：Hello PDU、LSP（Link-State PDU，链路状

态 PDU）和 SNP（Sequence Number PDU，序列号 PDU）这三种。

1．Hello PDU

与 OSPF 的 Hello 报文一样，IS-IS 的 Hello PDU 也是周期性地向邻居路由器发送的，也用于建立和维持邻居关系，称为 IIH（IS-to-IS Hello）。其中，广播网中 L1 邻居关系的建立和维护使用的是 L1 LAN IIH（类型号为 15）；广播网中 L2 邻居关系的建立和维护使用的是 L2 LAN IIH（类型号为 16）；非广播网络中则使用 P2P IIH（类型号为 17）。它们的报文格式有所不同，具体将在 13.2.3 小节介绍。

2．LSP PDU

LSP PDU 是包含 IS-IS 路由器链路状态信息的 PDU，用于与其他 IS-IS 路由器交换链路状态信息，类似于 OSPF 中的 LSA 报文。每个 IS-IS 路由器都会产生自己的 LSP，并向邻居路由器进行泛洪，同时又可以学习由邻居路由器泛洪而来的其他 IS-IS 路由器的 LSP。

LSP 也分为两种：L1 LSP（类型号为 18）和 L2 LSP（类型号为 20）。L1 LSP 可由 L1 或者 L1/2 IS-IS 路由器产生，L2 LSP 可由 L2 或者 L1/2 IS-IS 路由器产生。这些 LSP 是建立对应级别 LSDB 的依据。同一区域中各路由器上同级别的 LSDB 是完全同步的，而各级 LSDB 又是路由器通过 SPF 算法计算 SPT（最短路径树）、最终得出路由表的依据。

3．SNP PDU

SNP PDU 通过描述全部或部分数据库中的 LSP 来同步各 LSDB，从而维护相同区域中同级别 LSDB 的完整与同步，类似于 OSPF 中的 DD 报文。

SNP 又包括 CSNP（Complete SNP，完全序列号 PDU）和 PSNP（Partial SNP，部分序列号 PDU）。PSNP 只列举最近收到的一个或多个 LSP 的序号，能一次对多个 LSP 进行确认。同时，当发现自己的 LSDB 与对端邻居，或者广播网络中的 DIS 的 LSDB 不同步时，也是用 PSNP 来请求邻居或者 DIS 发送新的 LSP。CSNP 包括本地某个级别 LSDB 中所有 LSP 的摘要信息，从而可以在相邻路由器间保持同级别 LSDB 同步。在广播网络上，CSNP 由 DIS 定期发送（缺省的发送周期为 10 s）；在点对点线路上，CSNP 只在第一次建立邻接关系时发送。

CSNP 和 PSNP 分别也可分为 L1 CSNP（类型号为 24）、L2 CSNP（类型号为 25）、L1 PSNP（类型号为 26）和 L2 PSNP（类型号为 27）。

13.2.2　IS-IS PDU 报头格式

以上这些 IS-IS PDU 都包括一个报头和可变长字段两部分。报头又包括“通用报头”和“专用报头”。对所有 PDU 来说，通用报头是相同的，专用报头根据不同 PDU 类型而不同。总体的 IS-IS PDU 结构如图 13-7 所示。

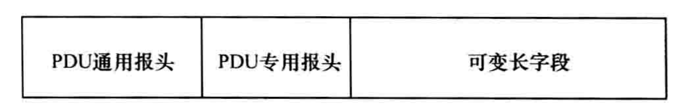


图 13-7　IS-IS PDU 基本结构

IS-IS PDU 通用报头格式如图 13-8 所示。各字段说明如下。

① Intradomain Routing Protocol Discriminator：域内路由协议标识符，占 1 个字节，用于标识网络层 PDU 的类型，IS-IS PDU 的固定值为 0x83。

② Length Indicator：长度指示器，占 1 个字节，用于标识报头部分（包括通用报头和各种 PDU 的专用报头两部分）长度，以字节为单位。

③ Version/Protocol ID Extension：版本/协议 ID 扩展，占 1 个字节，当前值固定为 0x01。

④ ID Length：ID 长度，占 1 个字节，用于标识系统 ID 长度。

⑤ PDU Type：PDU 类型，占 5 位，用于标识 IS-IS PDU 的类型。值为 15 表示 L1 LAN IIH；值为 16 表示 L2 LAN IIH；值为 18 表示 L1 LSP；值为 20 表示 L2 LSP；值为 24 表示 L1 CSNP；值为 25 表示 L2 CSNP；值为 26 表示 L1 PSNP；值为 27 表示 L2 CSNP。

⑥ Version：IS-IS 协议版本号，占 1 个字节，当前值为 0x01。

⑦ Reserved：保留位，占 1 个字节，当前值固定为 0。

⑧ Maximum Area Addresses：最多区域地址，占 1 个字节，标识支持的最大区域数，表示可以为一个路由器配置多少个不同的区域前缀。缺省值为 0，表示最多支持 3 个区域地址数。

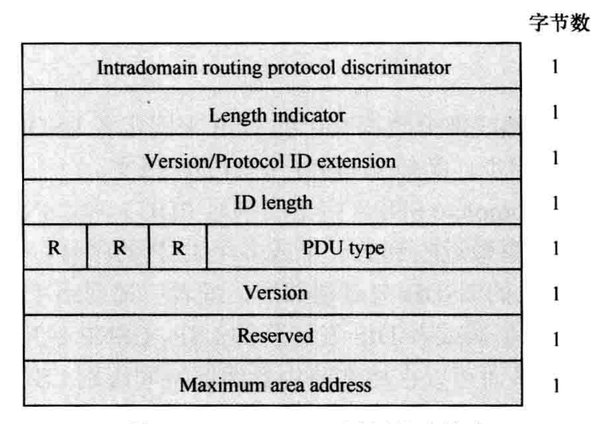


图 13-8 IS-IS PDU 通用报头格式

13.2.3 IIH PDU 报文格式

IIH（IS-IS Hello）PDU 用来建立和维持 IS-IS 路由器之间的邻接关系。IIH PDU 包括 IS-IS PDU 通用报头、IIH 专用报头和可变长字段三部分。在 IIH 专用报头部分包括了发送者的系统 ID、分配的区域地址和发送路由器已知的链路上邻居标识。另外，IIH 有以下三种类型。

① L1 LAN IS-IS Hello PDU（类型号为 15）：广播网中 L1 路由器发送的 IIH。

② L2 LAN IS-IS Hello PDU（类型号为 16）：广播网中 L2 路由器发送的 IIH。

③ 点对点 IS-IS Hello PDU（类型号为 17）：在点对点网络上路由器发送的 IIH。

前面两种统称为广播 LAN IIH，后面一种称为 P2P IIH。这些不同类型的 IIH 的 PDU 报文格式不完全一样，图 13-9 所示的是广播网中 L1 和 L2 路由器发送的 IIH 报文的格式，图 13-10 所示的是点对点网络中路由器发送的 IIH 报文的格式。通过比较可以发现，总

体来说，**P2P IIH 中相对于 LAN IIH 多了一个表示本地链路 ID 的 Local Circuit ID 字段，少了表示广播网中 DIS 的优先级的 Priority 字段以及表示 DIS 和伪节点 System ID 的 LAN ID 字段。**

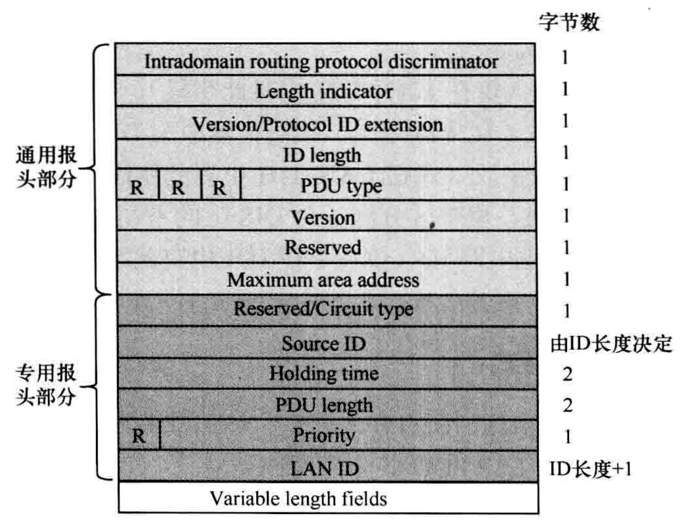


图 13-9　广播 LAN IIH 报文格式

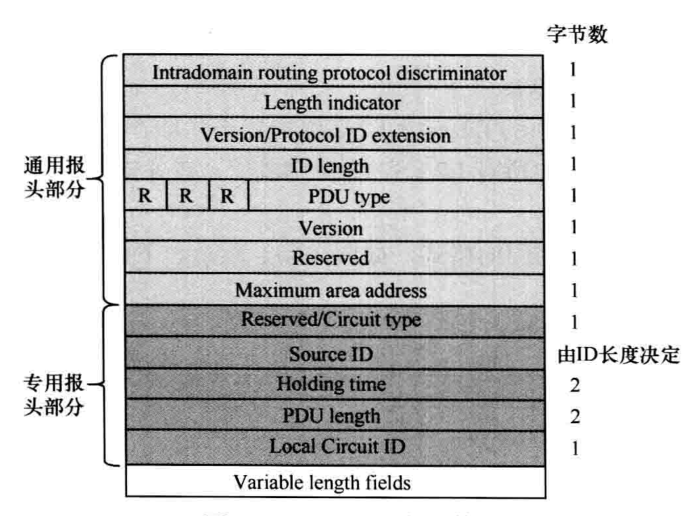


图 13-10　P2P IIH 报文格式

下面介绍这些 IIH PDU 专用报头部分的各个字段。

① Reserved：保留字段，占 6 位。当前没有使用，始终为 0。

② Circuit Type：电路类型字段，占 2 位。0x01 表示 L1 路由器，0x10 表示 L2 路由器，0x11 表示 L1/2 路由器。

③ Source ID：源 ID 字段，占 1 个字节，标识发送该 IIH PDU 报文的源路由器系统 ID。

④ Holding Time：保持时间，占 2 个字节，用来通知它的邻居路由器在认为这台路由器失效之前应该等待的时间。如果在保持时间内收到邻居发送的下一个 IIH PDU，将认为邻居依然处于存活状态。这个保持时间就相当于 OSPF 中的 DeadInterval（死亡时间

间隔)。在 IS-IS 中，缺省情况下保持时间是发送 IIH PDU 间隔的 3 倍，但是在配置保持时间时，是通过指定一个 IIH PDU 乘数（Hello-Multiplier）进行配置的。例如，如果 IIH PDU 的间隔为 10 s，IIH PDU 乘数为 3，那么保持时间就是 30 s。

⑤ PDU Length：IIH PDU 长度字段，占 2 个字节，标识整个 IIH PDU 报文（包括 IS-IS PDU 报头）的长度（以字节为单位）。

⑥ Priority：优先级字段（**仅在 LAN IIH 中有此字段**），占 7 位，标识本路由器在 DIS 选举中的优先级。值越大，优先级越高，该路由器成为 DIS 的可能性越大。

⑦ LAN ID：局域网 ID 字段（**仅在 LAN IIH 中有此字段**），由 DIS 路由器的系统 ID+1 个字节的伪节点 ID 组成，用来区分同一台 DIS 上的不同 LAN。

⑧ Local Circuit ID：本地电路 ID（**仅在 P2P IIH 中有此字段**），占 1 个字节，用来标识本地链路 ID。

13.2.4 LSP PDU 报文格式

一个 LSP 包含了一个路由器的所有基本信息，如邻接关系、连接的 IP 地址前缀、OSI 终端系统、区域地址等。LSP PDU 共分为两种类型。

1. L1 LSP（类型号为 18）

L1 LSP 是由支持 L1 路由的 L1 或者 L1/2 路由器产生的，会在本区域内部邻居路由器上泛洪。本区域中的所有 L1 LSP 交换完成后会在所有本区域 L1 或者 L1/2 路由器上形成完全一致的 L1 LSPDB。

2. L2 LSP（类型号为 20）

L2 LSP 是由支持 L2 路由的 L2 或者 L1/2 路由器产生的，在位于不同区域中的邻居路由器上泛洪。当整个网络中所有 L2 LSP 交换完成后，在各支持 L2 路由的路由器上会形成完全一致的 L2 LSPDB。

这两种 LSP PDU 具有相同的格式，如图 13-11 所示。下面是 LSP 专用报头部分各字段说明。

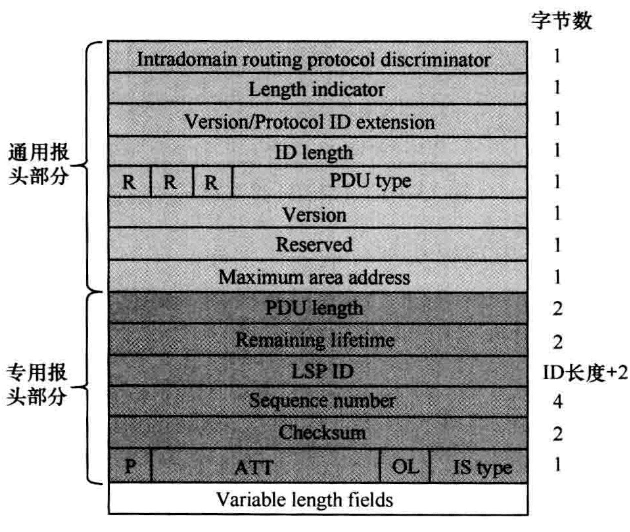


图 13-11 LSP PDU 报文格式

① PDU Length：LSP PDU 长度字段，占 2 个字节，标识整个 LSP PDU 报文的长度（包括通用报头）。

② Remaining Lifetime：剩余生存时间字段，占 2 个字节，标识此 LSP PDU 所剩的生存时间，单位为秒。当生存时间为 0 时，LSP 将被从链路状态数据库中清除。

③ LSP ID：LSP 标识符字段，占“系统 ID 长度+2”个字节，用来标识不同的 LSP PDU 和生成 LSP 的源路由器。它包括三部分：Source ID（源 ID，也即 System ID）、Pseudonode ID（伪节点 ID，简称“PN-ID”，普通路由器 LSP 的伪节点 ID 为 0，伪节点 LSP 的伪节点 ID 不为 0）和 LSP Number（LSP 序列号，即 LSP 的分片号，简称“Frag-Nr”）。图 13-12 所示为一个 LSP ID 示例，其中标注了各部分的组成。

00c0.0040.1234.02-00

SystemID　PN-ID　Frag-Nr

图 13-12　LSP ID 组成示例

④ Sequence Number：序列号字段，占 4 个字节，标识每个 LSP PDU 的序列号。每一个 LSP 都拥有一个标识自己的 4 字节的序列号。**它是针对本地路由器发送的 LSP 而言的**，在路由器启动时所发送的第一个 LSP 报文中的序列号为 1，以后当需要生成新的 LSP 时，新 LSP 的序列号在前一个 LSP 序列号的基础上加 1。更高的序列号意味着更新的 LSP。

⑤ Checksum：校验和字段，占 2 个字节，用于接收端校验传送的 LSP PDU 的完整性和正确性。当一台路由器收到一个 LSP 时，在将该 LSP 放入本地链路数据库和将其再泛洪给其他邻接路由器之前，会重新计算 LSP 的校验和，如果校验和与 LSP 中携带的校验和不一致，则说明此 LSP 传输过程中已经被破坏，不再泛洪。

⑥ P（Partition）：分区字段，占 1 位，表示区域划分或者分段区域的修复位，**仅与 L2 LSP 有关**。当 P 位被设置为 1 时，表明始发路由器支持自动修复区域的分段情况。

⑦ ATT（Attached）：区域关联字段，占 4 位，表示产生此 LSP PDU 的路由器与多个区域相连。虽然 ATT 位同时在 L1 LSP 和 L2 LSP 中进行了定义，但是它**只会在 L1/2 路由器的 L1 LSP 中被设置**。当 L1/2 路由器在 L1 区域内传送 L1 LSP 时，如果 L1 LSP 中设置了 ATT 位，则表示该区域中的 L1 路由器可以通过此 L1/2 路由器通往外部区域。

⑧ OL（Overload）：过载字段，占 1 位，置 1 时表示本路由器因内存不足而导致 LSDB 不完整。设置了过载标志位的 LSP 虽然还会在网络中扩散，但是在计算通过过载路由器的路由时不会被采用。即对路由器设置过载位后，其他路由器在进行 SPF 计算时不会使用这台路由器做转发，只计算该节点上的直连路由。

如 13-13 所示，RouterA 到 1.1.1.0/24 网段的报文由 RouterB 转发，但如果 RouterB 所发的 LSP 报文中过载标志位置 1，RouterA 会认为 RouterB 的 LSDB 不完整，于是将报文通过 RouterD、RouterE 转发到 1.1.1.0/24 网段，转发到 RouterB 直连网段的报文则不受影响。

当系统因为各种原因无法保存新的 LSP，以致无法维持正常的 LSDB 同步时，该系统计算出的路由信息将出现错误。在这种情况下，系统就可以自动进入过载状态，即通过该设备到达的路由不计算，但该设备的直连路由不会被忽略。

说明　除了设备异常可导致自动进入过载状态外，也可以通过手动配置使系统进入过载状态。当网络中的某些 IS-IS 设备需要升级或维护时，需要暂时将该设备从网络中隔离。

此时可以给该设备设置过载标志位，这样就可以避免其他设备通过该节点来转发流量。

如果因为设备进入异常状态导致系统进入过载状态，此时系统将删除全部引入或渗透的路由信息；而如果因为用户配置导致系统进入过载状态，此时会根据用户的配置决定是否删除全部引入或渗透路由。有关渗透路由将在 13.3.4 小节介绍。

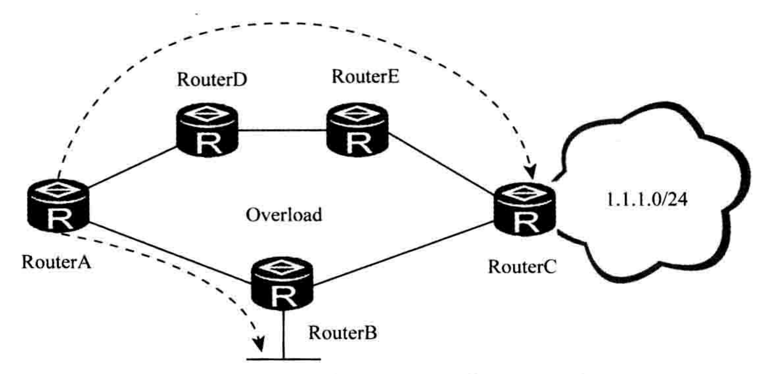


图 13-13　LSP PDU 中设置了 OL 标志位的应用示例

⑨ IS Type：路由器类型字段，占 2 位，用来指明生成此 LSP 的路由器类型是 L1 路由器还是 L2 路由器，也表示了收到此 LSP 的路由器将把这个 LSP 放在 L1 LSPDB 中还是放在 L2 LSPDB 中。01 表示 L1，11 表示 L2。

13.2.5 SNP PDU 报文格式

SNP 分为 CSNP 和 PSNP。它们的报文格式比较简单，CSNP PDU 报文格式如图 13-14 所示，PSNP PDU 报文格式如图 13-15 所示。这两种 SNP PDU 中专用报头部分的字段说明如下。

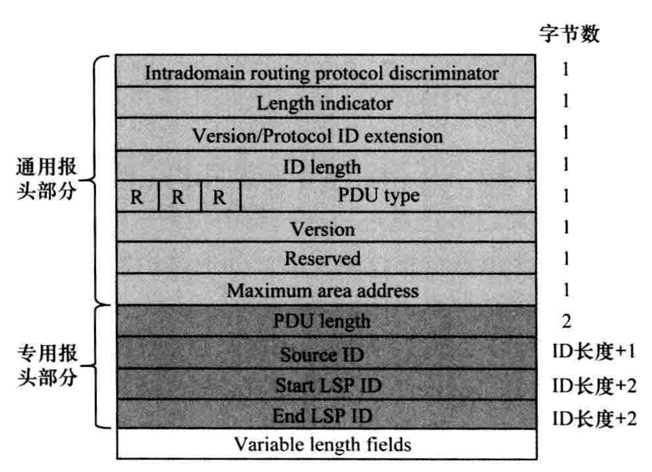


图 13-14　CSNP PDU 报文格式

① PDU Length：SNP PDU 长度字段，占 2 个字节，标识整个 SNP PDU 报文的长度（包括通用报头）。

② Source ID：源 ID 字段，占“系统 ID 长度+1”个字节，标识发送该 SNP PDU 的路由器的 System ID。

③ Start LSP ID：起始 LSP ID 字段（**仅 CSNP PDU 中有此字段**），占“系统 ID 长度+2”个字节，表示在下面的可变字段中描述的 LSP 范围中的第一个 LSP ID 号。

④ End LSP ID：结束 LSP ID 字段（**仅 CSNP PDU 中有此字段**），占“系统 ID 长度+2”个字节，表示在下面的可变字段中描述的 LSP 范围中的最后一个 LSP ID 号。

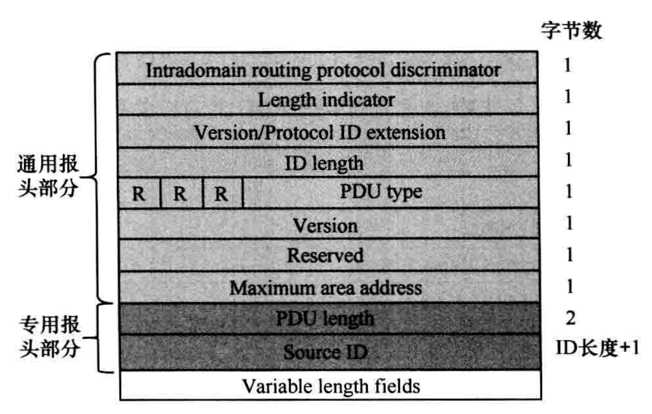


图 13-15　PSNP PDU 报文格式

13.2.6　IS-IS PDU 可变字段格式

从上面介绍的各种 PDU 报文格式可以看到，除了报头（包括通用报头和专用报头）部分之外，最后还有一个部分，就是“可变长字段”（Variable length fields）部分。这个“可变长字段”部分就是各种 PDU 报文的真正内容部分，是整个 PDU 报文的核心部分。因为这部分内容都是以“Type-Length-Value”（类型-长度-值）格式列出的，所以也称为“TLV”部分。

TLV 编址方式由三大部分组成：T（Type），即 PDU 报文类型，不同类型由不同的值定义；L（Length），即 Value 字段的长度，以字节为单位；V（Value），即包的真正内容，是最重要的部分）。但在 ISO10589 和 RFC1195 这两种当前 IS-IS 标准中，使用“code”（代码）替换了前面所说的“Type”部分，所以这种报文编址方式通常也称为 CLV（Code-Length-Value），如图 13-16 所示。这三个字段的说明如下。

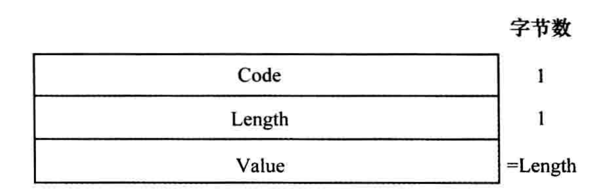


图 13-16　可变长字段部分格式

① Code：代码字段，占 1 个字节，表示 PDU 类型，不同的 IS-IS PDU 使用不同的类型，具体参见 13.2.1 小节相关说明。

② Length：长度字段，占 1 个字节，表示 Value 字段的长度，最大值为 255 字节。

③ Value：值字段，长度是可变的，表示实际承载的 PDU 内容，最大为 255 字节。

在 IS-IS PDU 使用的各种 TLV 中，既有 ISO 10589 中定义的，也有 RFC 1195 中定

义的。ISO 中定义的 TLV 用于 CLNP 网络环境，但是其中的大多数也用于 IP 网络环境。RFC 中定义的 TLV 只用于 IP 环境。也就是说，对于一个 IS-IS PDU，后面既可以携带支持 CLNP 的 TLV，又可以携带支持 IP 的 TLV。如果一个路由器不能识别一个 TLV，那么将忽略它。

不同 TVL 类型和各种 IS-IS PDU 的对应关系如表 13-1 所示。其中，Type 值从 1 到 10 的 TLV 在 ISO10589 中定义，其他几种 TLV 在 RFC1195 中定义。

表 13-1 TVL 类型与 IS-IS PDU 的对应关系

TLV Type	名称	所应用的 PDU 类型
1	Area Addresses	IIH、LSP
2	IS Neighbors（LSP）	LSP
4	Partition Designated Level2 IS	L2 LSP
6	IS Neighbors（MAC Address）	LAN IIH
7	IS Neighbors（SNPA Address）	LAN IIH
8	Padding	IIH
9	LSP Entries	SNP
10	Authentication Information	IIH、LSP、SNP
128	IP Internal Reachability Information	LSP
129	Protocols Supported	IIH、LSP
130	IP External Reachability Information	L2 LSP
131	Inter-Domain Routing Protocol Information	L2 LSP
132	IP Interface Address	IIH、LSP

13.3 IS-IS 基本原理

IS-IS 是一种链路状态路由协议，每一台路由器都会生成自己的 LSP（会不断更新的），它包含了该路由器所有使能 IS-IS 协议接口的链路状态信息。通过跟相邻设备建立 IS-IS 邻接关系，互相更新本地设备的 LSDB，可以使得 LSDB 与整个 IS-IS 网络的其他设备的 LSDB 实现同步。然后根据 LSDB 运用 SPF 算法计算出 IS-IS 路由。如果此 IS-IS 路由是到目的地址的最优路由，则此路由会下发到 IP 路由表中，并指导报文的转发。

13.3.1 IS-IS 邻居关系的建立

上一章介绍的 OSPF 协议支持 Braocast（广播）、P2P（点对点）、NBMA（非广播多路访问）、P2MP（点对多点）这 4 种主要网络类型，但 IS-IS 仅支持 Braocast（如以太网、令牌环网、FDDI）和 P2P（链路封装 PPP 或者 HDLC 协议的网络）这两种网络类型。若要在 NBMA 网络中使用（如 X.25、FR 和 ATM 网络），需要配置子接口，并配置子接口的类型为 P2P。IS-IS 不能在 P2MP 网络上运行。

1. IS-IS 邻居建立原则

IS-IS 按如下原则建立邻居关系。

① 只有同一层次（具体参见 13.1.5 小节）的相邻路由器才有可能成为邻居，**即只**

能建立单跳的邻居关系，不能跨路由器建立邻居关系。

② 对于 L1 路由器来说，区域号必须一致。

③ 链路两端 IS-IS 接口的网络类型必须一致。

说明　通过将以太网接口模拟成 P2P 接口，可以建立 P2P 链路邻居关系。

④ **链路两端 IS-IS 接口的 IP 地址必须处于同一网段。**

由于 IS-IS 是直接运行在数据链路层上的协议，并且最早设计是给 CLNP 使用的，因此 IS-IS 邻居关系的形成与 IP 地址无关。但在 IP 网络上运行 IS-IS 时，是需要检查对方的 IP 地址的。如果接口配置了从 IP，那么只要双方有某个 IP（**主 IP 或者从 IP**）在同一网段，就能建立邻居，不一定要与主 IP 相同。

说明　当链路两端 IS-IS 接口的 IP 地址不在同一网段时，如果配置接口对接收的 Hello 报文不做 IP 地址检查，也可以建立邻居关系。对于 P2P 接口，可以配置接口忽略 IP 地址检查；对于以太网接口，需要将以太网接口模拟成 P2P 接口，然后才可以配置接口忽略 IP 地址检查。

两台运行 IS-IS 的路由器在交互协议报文实现路由功能之前必须首先建立邻居关系。在不同类型的网络上，IS-IS 的邻居建立方式不相同，下面分别予以介绍。

2. 在广播链路上建立邻居关系

IS-IS 在广播链路上是采用二层组播方式发送 Hello 报文的，L1 IIH 报文发送到 01-80-C2-00-00-14 组播 MAC 地址，L2 IIH 发送到 01-80-C2-00-00-14 组播 MAC 地址。当邻居双方都收到了 Hello 报文后，它们之间的邻居关系就建立了。

总体来说，**IS-IS 在广播链路上需要进行三次握手验证，邻居关系才可以建立。**在这一点上与 OSPF 广播类型网络邻居的建立是一致的。但要注意的是，OSPF 是以 IP 协议封装的，所以是以组播 IP 地址发送 Hello 报文，而 IS-IS 是链路层协议，直接以帧发送，是通过组播 MAC 地址发送的，里面封装的是邻居的 SNPA（Subnetwork Point of Attachment，子网连接点）地址。

下面以 L2 路由器为例介绍广播链路中建立邻居关系的过程，如图 13-17 所示。L1 路由器之间建立邻居与此相同。在此假设 RouterA 的 IS-IS 接口先使能 IS-IS。

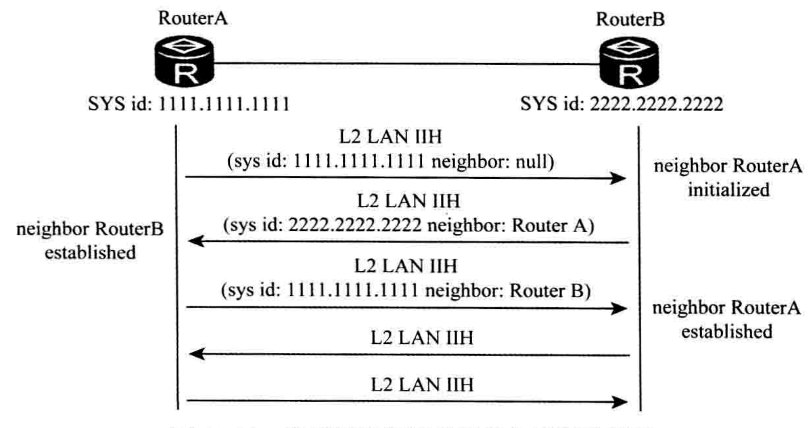


图 13-17　广播链路邻居关系建立流程示意图

① 在 RouterA 连接 RouterB 的接口使能 IS-IS 协议后，立即以组播方式发送 L2 LAN IIH（因为此处是假设 RouterA 和 RouterB 均为 L2 路由器），此时报文中包含一个 LAN ID、那就是 DIS，另外报文中的 IS Neighbors（SNPA Address）TLV 字段（参见 13.2.6 小节的表 13-1）没有邻居的 SNPA 地址（通常是映射成路由器的主机名），因为还没收到邻居的 Hello 报文。

② RouterB 收到此报文后会进行系列的校验动作，如 System ID 长度是否匹配、Max Area Address 是否匹配、验证密码（配置报文验证时）是否正确等。通过检验后，将自己和 RouterA 的邻居状态标识为 Initial（初始化）状态。然后，从 IIH 报文中 Source ID 字段中获取 RouterA 的 System ID，添加到邻居表中。再向 RouterA 回复 L2 LAN IIH 报文，报文中的 IS Neighbors（SNPA Address）TLV 字段为 RouterA 的 SNPA 地址，标识 RouterA 为自己的邻居。

③ 在 RouterA 收到此报文后，发现报文中有自己的 SNPA 地址，于是将自己与 RouterB 的邻居状态标识为 Up，将 RouterB 的 System ID 添加到自己的邻居表中，标识 RouterB 为自己的邻居。然后 RouterA 再向 RouterB 发送一个在 IS Neighbors（SNPA Address）TLV 字段中标识 RouterB 的 SNPA 地址的 L2 LAN IIH 报文。

④ 在 RouterB 收到此报文后，发现有自己的 SNPA 地址，于是将自己与 RouterA 的邻居状态标识为 Up。这样，两个路由器成功建立了邻居关系。

因为是广播网络，需要选举 DIS，所以在邻居关系建立后，路由器会等待两个 Hello 报文间隔，再进行 DIS 的选举。Hello 报文中包含 Priority 字段，Priority 值最大的将被选举为该广播网的 DIS。如果优先级相同，接口 MAC 地址较大的被选举为 DIS。

3. P2P 链路邻居关系的建立

在 P2P 链路上，邻居关系的建立不同于广播链路，**分为两次握手机制和三次握手机制**。在两次握手机制中，只要路由器收到对端发来的在 IS Neighbors（SNPA Address）TLV 字段中包含自己 SNPA 地址的 Hello 报文，就单方面宣布邻居为 Up 状态，建立邻居关系。而在三次握手机制中，需要通过三次发送 P2P 的 IS-IS Hello PDU 才能最终建立起邻居关系，类似广播链路上邻居关系的建立，参见图 13-17，不同的只是在 P2P 链路上发送的是 P2P IIH 报文，而不是 LAN IIH 报文。

两次握手机制存在明显的缺陷。当路由器间存在两条及以上的链路时，如果某条链路上到达对端的单向状态为 Down，而另一条链路同方向的状态为 Up，路由器之间还是能建立起邻接关系。SPF 在计算时会使用状态为 UP 的链路上的参数，这就导致没有检测到故障的路由器在转发报文时仍然试图通过状态为 Down 的链路。三次握手机制解决了上述不可靠点到点链路中存在的问题。这种方式下，路由器只有在知道邻居路由器也接收到它的报文时，才宣布邻居路由器处于 Up 状态，从而建立邻居关系。

13.3.2 IS-IS 的 LSP 交互过程

IS-IS 路由域内的所有路由器都会产生自己的 LSP，当发生以下事件时会触发一个新的 LSP。

① 邻居 Up 或 Down。

② IS-IS 相关接口 Up 或 Down。

③ 引入的 IP 路由发生变化。

④ 区域间的 IP 路由发生变化。

⑤ 接口被赋了新的 metric 值。

⑥ 周期性更新。

在收到邻居新的 LSP 后，将接收的新的 LSP 合并到自己的 LSDB 中，并标记为 flooding（泛洪），发送新的 LSP 到除了收到该 LSP 的接口之外的接口。邻居收到后再扩散到它们的邻居，一级级地扩散，最终实现整个 IS-IS 网络中各路由器的 LSDB 同步。

说明 LSP 报文的“泛洪”（flooding）是指当一个路由器向相邻路由器通告自己的 LSP 后，相邻路由器再将同样的 LSP 报文传送到除发送该 LSP 的路由器外的其他邻居，并这样逐级将 LSP 传送到整个层次内所有路由器的一种方式。通过这种“泛洪”，整个层次内的每一个路由器就都可以拥有相同的 LSP 信息，并保持 LSDB 的同步。

每一个 LSP 都拥有一个标识自己的 4 字节的序列号。在路由器启动时所发送的第一个 LSP 报文中的序列号为 1，以后当需要生成新的 LSP 时，新 LSP 的序列号在前一个 LSP 序列号的基础上加 1。更高的序列号意味着更新的 LSP。

1. 广播链路中新加入路由器与 DIS 同步 LSDB 的过程

下面以图 13-18 为例介绍广播链路中新加入路由器与 DIS 同步 LSDB 的流程。假设 RouterC 是新加入的。

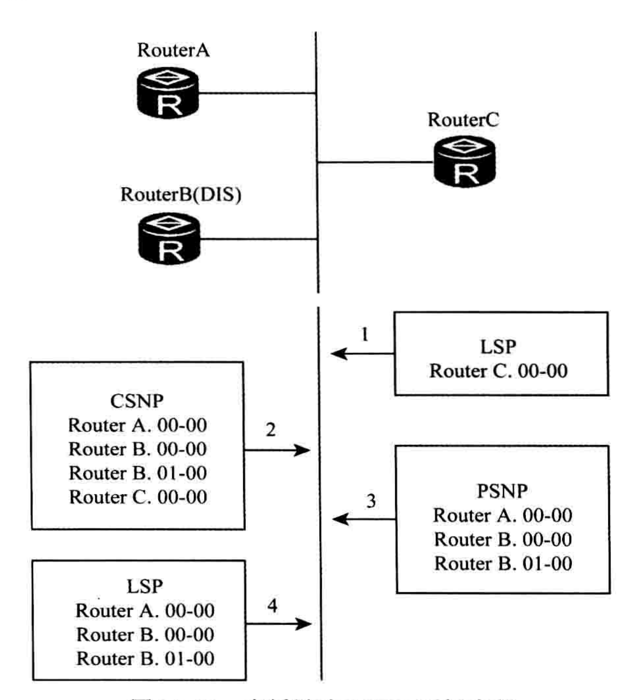


图 13-18　广播链路 LSDB 更新流程

① 新加入的路由器 RouterC 首先发送 Hello 报文，与该广播域中的路由器建立邻居关系。

② 建立邻居关系之后，RouterC 等待 LSP 刷新定时器超时，然后将自己的 LSP 发

往组播地址（L1 LSP 发送到 01-80-C2-00-00-14 组播地址；L2 LSP 发送到 01-80-C2-00-00-15 组播地址，参见图中的 1 号报文）。这样网络上的所有邻居都将收到该 LSP。

③ 该网段中的 DIS 会把收到 RouterC 的 LSP 加入 LSDB 中，并等待 CSNP 报文定时器超时并向网络内广播 CSNP 报文（参见图中的 2 号报文），进行该网络内的 LSDB 同步。而其他邻居在收到 RouterC 发来的 LSP 时会直接丢弃，因为在广播网络中，区域内的路由器只能与 DIS 进行 LSP 交互。

④ RouterC 收到 DIS 发来的 CSNP 报文，对比自己的 LSDB 数据库，发现有许多 LSP 在本地数据库中没有，于是向 DIS 发送 PSNP 报文（参见图中的 3 号报文）请求自己没有的 LSP。

⑤ DIS 收到该 PSNP 报文请求后向 RouterC 发送对应的 LSP（参见图中的 4 号报文）进行 LSDB 的同步。

如果不是新路由器加入，在正常的 LSP 更新中，DIS 的 LSDB 更新过程如下。

① DIS 接收到 LSP 后在自己的 LSDB 中搜索对应的记录。如果没有该 LSP（每个 IS-IS 路由器都有自己的 LSP，通过 LSP ID 中的 System ID 部分进行区分，**每个路由器的 System ID 是唯一的**），则将其加入数据库，并在网络内广播新的 LSP。

② 如果收到的 LSP 序列号大于本地已有的对应路由器的 LSP 的序列号，就替换为新的 LSP 报文，并在网络中泛洪新的 LSP 报文；如果收到的 LSP 序列号小于本地已有的对应路由器的 LSP 的序列号，则向入端接口发送本地已有的对应路由器的 LSP 报文，使对端更新 LSDB。

③ 如果新接收的 LSP 与本地已有对应的路由器的 LSP 序列号相等，则比较两 LSP 报文中的 Remaining Lifetime（存活时间）字段值。如果新收到的 LSP 的 Remaining Lifetime 大于本地已有对应路由器的 LSP 的 Remaining Lifetime，就替换为新报文，并广播新数据库内容，否则就向入端接口发送本地已有的对应路由器的 LSP 报文，使对端更新 LSDB。

④ 如果新接收的 LSP 与本地已有对应的路由器的 LSP 的序列号和 Remaining Lifetime 都相等，则比较两个 LSP 的 Checksum 字段值。如果新收到的 LSP 的 Checksum 大于本地已有对应的路由器的 LSP 的 Checksum，就替换为新的 LSP 报文，并在网络泛洪新的 LSP，否则就向入端接口发送本地已有的对应路由器的 LSP 报文，使对端更新 LSDB。

⑤ 如果两个 LSP 的序列号、Remaining Lifetime 和 Checksum 都相等，则不转发该报文。

2. P2P 链路上 LSDB 数据库的同步过程

在 P2P 链路中不存在 DIS，LSDB 的同步、更新是在链路两端的路由器上进行的。下面以图 13-19 为例介绍 P2P 链路上 LSDB 的同步与更新流程。先介绍 LSDB 的同步流程。

① RouterA 先与 RouterB 建立邻居关系。

② 建立邻居关系之后，RouterA 与 RouterB 会先发送各自的 CSNP 给对端设备。如果一方发现自己的 LSDB 没有与接收到的 CSNP 同步（里面的数据库内容存在不一致的地方），则该方向另一方发送 PSNP 报文，请求索取相应的 LSP。

③ 现假定 RouterB 通过 PSNP 报文向 RouterA 索取某些所需的 LSP，RouterA 在收

到该 PSNP 报文后，向 RouterB 发送所请求的 LSP，同时启动 LSP 重传定时器，并等待 RouterB 发来用作收到确认的 PSNP 报文。

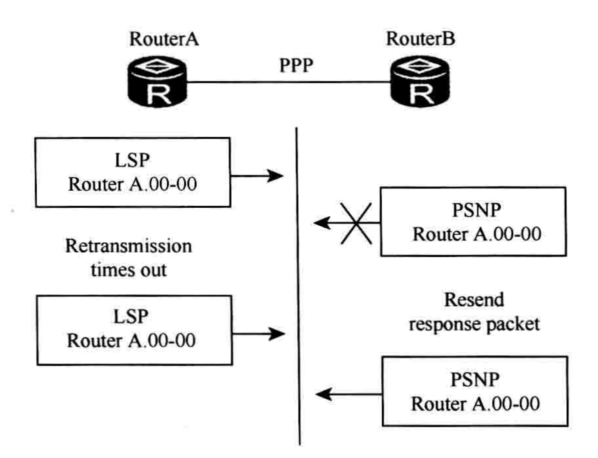


图 13-19　P2P 链路 LSDB 数据库同步流程

④ 如果在 LSP 重传定时器超时后，RouterA 还没有收到 RouterB 发送的 PSNP 报文作为应答，则重新发送原来已发送的对应 LSP，直至收到了来自 RouterA 的 PSNP 报文。

说明 从以上过程可以看出，在 P2P 链路上的 PSNP 报文有两种作用：一是用来向对方请求所需的 LSP，二是作为 Ack 应答以确认收到的 LSP。

在网络稳定时，在 P2P 链路中设备的 LSDB 更新过程如下。

① 如果新收到的 LSP 序列号比本地已有的对应路由器的 LSP 序列号更小，则直接给对方发送本地已有的对应路由器的 LSP，然后等待对方给自己一个 PSNP 报文作为确认；如果新收到的 LSP 比本地已有的对应路由器的 LSP 序列号更大，则将这个新的 LSP 存入自己的 LSDB，再通过一个 PSNP 报文来确认收到此 LSP，最后将这个新 LSP 以广播方式发送给除了发送该 LSP 的邻居以外的邻居。

② 如果收到的 LSP 序列号和本地已有的对应路由器 LSP 序列号相同，则比较它们的 Remaining Lifetime 字段值。如果新收到 LSP 的 Remaining Lifetime 小于本地已有的对应路由器的 LSP 的 Remaining Lifetime，则将新收到的 LSP 存入 LSDB 中，并发送 PSNP 报文来确认收到此 LSP，然后将该 LSP 发送给除了发送该 LSP 的邻居以外的邻居；如果新收到 LSP 的 Remaining Lifetime 大于本地已有的对应路由器的 LSP 的 Remaining Lifetime，则直接给对方发送本地已有的 LSP，然后等待对方给自己一个 PSNP 报文作为确认。

③ 如果新收到的 LSP 和本地已有的对应路由器的 LSP 的序列号和 Remaining Lifetime 都相同，则比较它们的 Checksum 字段值，如果收到 LSP 的 Checksum 大于本地已有的对应路由器的 LSP 的 Checksum，则将新收到的 LSP 存入 LSDB 中，并发送 PSNP 报文来确认收到此 LSP，然后将该 LSP 发送给除了发送该 LSP 的邻居以外的邻居；如果收到 LSP 的 Checksum 小于本地 LSP 的 Checksum，则直接给对方发送本地已有的对应路由器的的 LSP，然后等待对方给自己一个 PSNP 报文作为确认。

④ 如果收到的 LSP 和本地已有的对应路由器的 LSP 的序列号、Remaining Lifetime 和 Checksum 都相同，则不转发该报文。

13.3.3 IS-IS 报文验证

IS-IS 验证是基于网络安全性的要求而实现的一种验证手段，通过在 IS-IS 报文中增加验证字段对报文进行验证。当本地路由器接收到远端路由器发送过来的 IS-IS 报文时，如果发现验证密码不匹配，则将收到的报文丢弃，达到自我保护的目的。

1. IS-IS 验证的分类

根据报文的种类，IS-IS 验证可以分为以下三类。

① 接口验证：是指使能 IS-IS 协议的接口以指定方式和密码对 L1 和 L2 的 Hello 报文进行验证。对于 IS-IS 接口验证，有以下两种设置。

- 发送带验证 TLV 的验证报文，本地对收到的报文也进行验证检查。
- 发送带验证 TLV 的验证报文，但是本地对收到的报文不进行验证检查。

② 区域验证：是指在运行 IS-IS 的区域内部以指定方式和密码对 L1 的 SNP 和 LSP 报文进行验证。

③ 路由域验证：是指在运行 IS-IS 的路由域内部不同区域间以指定方式和密码对 L2 的 SNP 和 LSP 报文进行验证。

说明 对于区域和路由域验证，可以设置为 SNP 和 LSP 分开验证。

① 本地发送的 LSP 报文和 SNP 报文都携带验证 TLV，对收到的 LSP 报文和 SNP 报文都进行验证检查。

② 本地发送的 LSP 报文携带验证 TLV，对收到的 LSP 报文进行验证检查；发送的 SNP 报文携带验证 TLV，但不对收到的 SNP 报文进行检查。

③ 本地发送的 LSP 报文携带验证 TLV，对收到的 LSP 报文进行验证检查；发送的 SNP 报文不携带验证 TLV，也不对收到的 SNP 报文进行验证检查。

④ 本地发送的 LSP 报文和 SNP 报文都携带验证 TLV，对收到的 LSP 报文和 SNP 报文都不进行验证检查。

根据报文的验证方式，可以分为以下三类。

① 明文验证：一种简单的验证方式，将配置的密码直接加入报文中，这种验证方式安全性不够。

② MD5 验证：通过将配置的密码进行 MD5 算法摘要之后再加入报文中，这样提高了密码的安全性。

③ Keychian 验证：通过配置随时间变化的密码链表来进一步提升网络的安全性。

2. 验证信息的携带形式

IS-IS 是通过 TLV 的形式携带验证信息，验证 TLV 的类型为 10，具体格式如下。

① Type：ISO 定义验证报文的类型值为 10，长度为 1 字节。

② Length：指定验证 TLV 值的长度，长度 1 字节。0 为保留的类型，1 为明文验证，54 为 MD5 验证，255 为路由域私有验证方式。

③ Value：指定验证的类型和密码，长度为 1～254 字节。

13.3.4 IS-IS 路由渗透

在 IS-IS 协议中规定，L1 区域必须且只能与 L2 区域相连，不同的 L1 区域之间不直接相连。L1 区域内的路由信息可通过 L1/2 路由器发布到 L2 区域，因此，L2 路由器知道整个 IS-IS 路由域的路由信息。但是在缺省情况下，L2 路由器并不将自己知道的其他 L1 区域以及 L2 区域的路由信息发布到自己所连接的 L1 区域。这样该 L1 区域中的路由器将不了解本区域以外的路由信息，只将去往其他区域的报文发送到最近的 L1/2 路由器，可能导致对本区域之外的目的地址无法选择最佳的路由。另外，不同的 L1/2 到达目的的开销又可能相差很大，而 L1 路由器在选择 L1/2 路由器时仅考虑它们之间的链路开销。

为解决上述问题，IS-IS 提供了路由渗透（Route Leaking）功能，人为地把骨干网（即 L2 区域）的路由信息注入到普通的 L1 区域，保证普通区域也拥有整个 IS-IS 路由域的路由信息。路由渗透特性可以将 L2 的 IP 路由引入到 L1 路由器中去，这样可以允许 L1 路由器对某些或全部的 L2 路由选择出区域的最佳路径。当然也增加了区域内路由器的路由表规模。

IS-IS 路由渗透功能是通过在 L1/2 路由器上定义 ACL、路由策略、Tag 标记等方式，将符合条件的路由筛选出来，来实现将其他 L1 区域和 L2 区域的部分路由信息通报给自己所在 L1 区域的目的。

如图 13-20 所示，RouterA 发送报文给 RouterF，选择的最佳路径应该是 RouterA→RouterB→RouterD→RouterE→RouterF。因为这条链路上的 cost 值为 10+10+10+10=40，但在 RouterA 上查看发送到 RouterF 的报文选择的路径是：RouterA→RouterC→RouterE→RouterF，其 cost 值为 10+50+10=70，不是 RouterA 到 RouterF 的最优路由。

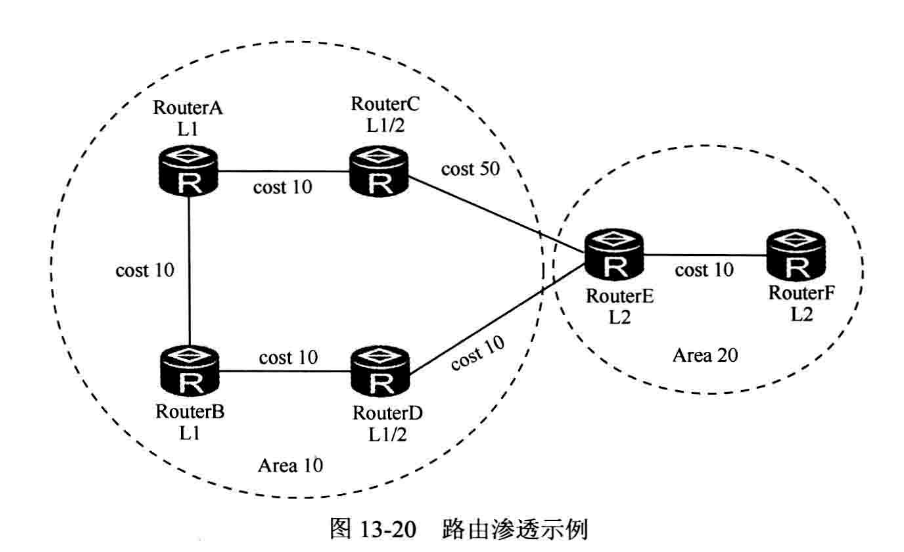


图 13-20　路由渗透示例

RouterA 作为 L1 路由器并不知道本区域外部的路由，那么发往区域外的报文都会选择由最近的 L1/2 路由器产生的缺省路由发送，所以会出现 RouterA 选择次最优路由转发报文的情况。

如果分别在 L1/2 路由器 RouterC 和 RouterD 上使能路由渗透功能，Aera10 中的 L1 路由器就会拥有经过这两个 L1/2 路由器通向区域外的路由信息。经过路由计算，选择的转发路径为 RouterA→RouterB→RouterD→RouterE→RouterF，即 RouterA 到 RouterF 的最优路由。

13.3.5 IS-IS 网络收敛

在 IS-IS 网络收敛方面，有快速收敛和按优先级收敛两种方式。快速收敛侧重于从路由的计算角度加快收敛速度；按优先级收敛侧重于从路由优先级角度提高网络性能。

1. 快速收敛

IS-IS 快速收敛是为了提高路由的收敛速度而提出的扩展特性。它包括以下几个功能。

（1）I-SPF

I-SPF（Incremental SPF，增量最短路径优先算法）是指当网络拓扑改变的时候，只对受影响的节点进行路由计算，不对全部节点重新进行路由计算，从而加快了路由的计算。

在 ISO10589 中定义使用 SPF 算法进行路由计算。当网络拓扑中有一个节点发生变化时，这种算法需要重新计算网络中的所有节点，计算时间长，占用过多的 CPU 资源，影响整个网络的收敛速度。而 I-SPF 改进了这个算法，除了第一次计算时需要计算全部节点外，后面的每次计算只需计算受到影响的节点，而最后生成的最短路径树 SPT 与原来的算法所计算的结果相同，大大降低了 CPU 的占用率，提高了网络收敛速度。

（2）PRC

PRC（Partial Route Calculation，部分路由计算）是指当网络上路由发生变化的时候，只对发生变化的路由进行重新计算。

PRC 的原理与 I-SPF 相同，都是只对发生变化的路由进行重新计算。不同的是，PRC 不需要计算节点路径，而是根据 I-SPF 算出来的 SPT 来更新路由。

在路由计算中，叶子代表路由，节点则代表路由器。如果 I-SPF 计算后的 SPT 改变，PRC 会只处理那个变化的节点上的所有叶子；如果经过 I-SPF 计算后的 SPT 并没有变化，则 PRC 只处理变化的叶子信息。比如一个节点使能一个 IS-IS 接口，则整个网络拓扑的 SPT 是不变的，这时 PRC 只更新这个节点的接口路由，从而降低 CPU 占用率。

PRC 和 I-SPF 配合使用可以将网络的收敛性能进一步提高，它是原始 SPF 算法的改进，已经代替了原有的算法。

（3）智能定时器

是在进行 SPF 计算和产生 LSP 的时候用到的一种智能定时器。该定时器的首次超时时间是一个固定的时间。如果在定时器超时前，又有触发定时器的事件发生，则该定时器下一次的超时时间会增加。

改进了路由算法后，如果触发路由计算的时间间隔较长，同样会影响网络的收敛速度。使用毫秒级定时器可以缩短这个间隔时间，但如果网络变化比较频繁，又会过度占用 CPU 资源。SPF 智能定时器既可以对少量的外界突发事件进行快速响应，又可以避免过度地占用 CPU。通常情况下，一个正常运行的 IS-IS 网络是稳定的，发生大量网络变动的机率很小，IS-IS 不会频繁地进行路由计算，所以第一次触发的时间可以设置得非常

短（毫秒级）。如果拓扑变化比较频繁，智能定时器随着计算次数的增加，间隔时间也会逐渐延长，从而避免占用大量的 CPU 资源。

与 SPF 智能定时器类似的还有 LSP 生成智能定时器。在 IS-IS 协议中，当 LSP 生成定时器到期时，系统会根据当前拓扑重新生成一个自己的 LSP。原有的实现机制是采用间隔时间固定的定时器，这样就不能同时满足快速收敛和低 CPU 占用率的需要。为此，将 LSP 生成定时器也设计成智能定时器，使其可以对突发事件（如接口 Up/Down）快速响应，加快网络的收敛速度，同时，当网络变化频繁时，智能定时器的间隔时间会自动延长，避免过度占用 CPU 资源。

（4）LSP 快速扩散

此特性可以加快 LSP 的扩散速度。

正常情况下，当 IS-IS 收到其他路由器发来的 LSP 时，如果此 LSP 比本地 LSDB 中相应的 LSP 要新，则更新 LSDB 中的 LSP，并用一个定时器定期将 LSDB 内已更新的 LSP 扩散出去。

LSP 快速扩散特性改进了这种方式，使能了此特性的设备收到一个或多个较新的 LSP 时，在路由计算之前，先将小于指定数目的 LSP 扩散出去，加快 LSDB 的同步过程。这种方式在很大程度上可以提高整个网络的收敛速度。

2. 按优先级收敛

IS-IS 按优先级收敛是指在大量路由情况下，能够让某些特定的路由（例如匹配指定 IP 前缀的路由）优先收敛的一种技术。因此用户可以把和关键业务相关的路由配置成相对较高的优先级，使这些路由更快地收敛，从而使关键的业务受到的影响减小。通过对不同的路由配置不同的收敛优先级，达到重要的路由先收敛的目的，提高网络的可靠性。

13.4　IS-IS 基本功能配置与管理

只有配置了 IS-IS 基本功能，才可组建 IS-IS 网络，才可以进行本章后面其他的配置。

IS-IS 基本功能包括以下几项配置任务。创建 IS-IS 进程是配置网络实体名称、配置全局 Level 级别以及建立 IS-IS 邻居的前提。在配置 IS-IS 基本功能之前，还需要配置接口 IP 地址，使相邻节点的网络层可达。

① 创建 IS-IS 进程。

② 配置网络实体名称。

③ 配置全局 Level 级别。

④ 建立 IS-IS 邻居。

⑤（可选）配置 IS-IS 主机名映射。

13.4.1　创建 IS-IS 进程

创建 IS-IS 进程是进行所有 IS-IS 配置的前提。IS-IS 支持多进程，它是指在同一个 VPN 下（或者同在公网下）可以创建多个 IS-IS 进程，每个进程之间互不影响，彼此独立。不同进程之间的路由信息交互相当于不同路由协议之间的路由交互。**但 IS-IS 进程**

也仅针对本地路由器而言，链路由两端的 IS-IS 进程号可以一样，也可以不一样。

IS-IS 多进程允许为一个指定的 IS-IS 进程关联一组接口，从而保证该进程进行的所有协议操作都仅限于这一组接口。这样，就可以使一台路由器有多个 IS-IS 协议进程，每个进程负责唯一的一组接口。创建 IS-IS 进程的方法很简单，具体步骤如表 13-2 所示。

表 13-2　　创建 IS-IS 进程的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**isis** [*process-id*] [**vpn-instance** *vpn-instance-name*] 例如：[Huawei] **isis** 10	创建 IS-IS 进程，使能 IS-IS 协议，并进入 IS-IS 视图。命令中的参数说明如下 ● *process-id*：可选参数，指定要创建的 IS-IS 进程号，取值范围为 1～65 535 的整数。如果不指定本参数，则直接创建并启动 IS-IS 1 进程 ● **vpn-instance** *vpn-instance-name*：可选参数，指定报建的 IS-IS 所属的 VPAN 实例的名称，1～31 个字符，区分大小写，不支持空格。如果不指定本参数，则创建的 IS-IS 进程属于公网 缺省情况下，未创建 IS-IS 进程，也没有使能 IS-IS 协议，可用 **undo isis** *process-id* 命令删除指定的 IS-IS 进程，去使能该进程下的 IS-IS 协议 【说明】一个 IS-IS 进程只能绑定到一个 VPN 上，一个 VPN 可以绑定多个 IS-IS 进程。VPN 实例删除时，与该 VPN 绑定的 IS-IS 进程也将被删除 必须在创建 IS-IS 进程时绑定 VPN 实例，否则无法通过配置将一个已存在的 IS-IS 进程绑定到一个 VPN 实例上
3	**description** *description* 例如：[Huawei-isis-10] **description** this process configure the area-authentication-mode	（可选）配置 IS-IS 进程的描述信息，可以方便地识别特殊进程，便于维护。参数 *description* 用来指定 IS-IS 进程的描述信息，取值范围为 1～80 个字符，区分大小写，支持空格 【说明】使用本命令配置的 IS-IS 进程描述信息，不会在 LSP 中发布，但使用 **is-name** *symbolic-name* 命令配置的 IS-IS 进程描述信息，会在 LSP 中发布 缺省情况下，不配置 IS-IS 进程的描述信息，可用 **undo description** 命令删除对应 IS-IS 进程下的描述信息

13.4.2 配置网络实体名称

网络实体名称 NET 是 NSAP 的特殊形式，由三部分组成：区域 ID（Area ID），区域 ID 的长度可以是变化的（1～13 个字节）；系统 ID（System ID），长度为固定值 6 个字节；最后一个字节 SEL，其值必须为 00。其中的系统 ID 用于识别不同的 IS-IS 路由器。

通常情况下，一个 IS-IS 进程下配置一个 NET 即可。当需要重新划分区域时，例如要将多个区域合并，或者将一个区域划分为多个区域，这种情况下配置多个 NET 可以在重新配置时仍然能够保证路由的正确性。由于在一个 IS-IS 进程中一台路由器的区域地址最多可配置 3 个，所以一台路由器在一个进程中的 NET 最多也只能配 3 个。在一个 IS-IS 路由器上配置多个 NET 时，必须保证它们的 System ID 部分都相同。**只有在完成 IS-IS 进程的 NET 配置后，IS-IS 协议才能真正启动。**

配置网络实体名的方法很简单，只需在对应的 IS-IS 进程视图下使用 **network-entity** *net* 命令配置即可。参数 *net* 用来指定本地路由器在对应进程下的网络实体名称，格式为 X…X.XXXX.XXXX.XXXX.00（都是十六进制的数），前面的“X…X”（1～13 个字节）是区域地址，中间的 12 个“X”（共代表 6 个字节）是路由器的 System ID，最后的“00”（1 个字节）是 SEL。

区域 ID 用来唯一标识路由域中的不同区域，同一 L1 区域内所有路由器必须具有相同的区域地址，L2 区域内的路由器可以具有不同的区域地址，具体要根据对应路由器所位于的区域。但在整个 L1 区域和 L2 区域中，每台路由器的系统 ID 必须保持唯一。**IS-IS 在建立 L2 邻居时，不检查区域地址是否相同，而在建立 L1 邻居时，区域地址必须相同，否则无法建立邻居。**

说明　为了避免冲突，可将路由器上的一个 Loopback 接口的 IP 地址转化为 NET 中的系统 ID 部分（最后 2 个用 0 补足），以保证 NET 在整个 IS-IS 进程下网络中的唯一性。如一个 Loopback 接口的 IP 地址为 1.1.1.1，则转换成系统 ID 为 0001.0001.0001.0000（注意要把 IP 地址中的十进制转换成十六进制）。也可事先编排好各路由器的系统 ID 部分，如分别用 0001.0001.0001、0002.0002.0002、0003.0003.003……如果网络中的 NET 不唯一，容易引发路由振荡，因此要做好前期网络规划。

缺省情况下，IS-IS 进程没有配置 NET，可用 **undo network-entity** *net* 命令删除 IS-IS 进程下指定的 NET。

【示例】指定 IS-IS 进程 1 的 NET 为 10.0001.1010.1020.1030.00。其中系统 ID 是 1010.1020.1030，区域 ID 是 10.0001。

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] network-entity 10.0001.1010.1020.1030.00
```

13.4.3　配置全局 Level 级别

建议在设计 IS-IS 网络之初就全局规划好各路由器的 Level 级别，也就是配置 IS-IS 路由器类型。在配置设备的 Level 级别时要充分考虑以下几个方面。

① 当 Level 级别为 L1 时，设备只与属于同一区域的 L1 和 L1/2 设备形成邻居关系，并且只负责维护 L1 的链路状态数据库 LSDB。

② 当 Level 级别为 L2 时，设备可以与同一或者不同区域的 L2 设备或者其他区域的 L1/2 设备形成邻居关系，并且只维护一个 L2 的 LSDB。

③ 当 Level 级别为 L1/2 时，设备会为 L1 和 L2 分别建立邻居，分别维护 L1 和 L2 两份 LSDB。

一般来说，将 L1 路由器部署在区域内，L2 路由器部署在区域间，L1/2 路由器部署在 L1 和 L2 路由器的中间。IS-IS 路由器的 Level 级别和接口的 Level 级别共同决定了建立邻居关系的 Level 级别。两台 L1/2 路由器建立邻居关系时，缺省情况下，会分别建立 L1 和 L2 邻居关系。如果只希望建立 L1 或者 L2 的邻居关系，可以通过执行 **isis circuit-level** [**level-1** | **level-1-2** | **level-2**]命令修改接口的 Level 级别来实现。

如果只有一个区域，建议用户将所有路由器的 Level 全部设置为 L1 或者全部设为

L2，因为没有必要让所有路由器同时维护两个完全相同的数据库。在 IP 网络中使用时，建议将所有的路由器都设置为 L2，这样有利于以后的扩展。

配置设备的 Level 级别的方法很简单，只需在对应的 IS-IS 进程下使用 **is-level** { **level-1** | **level-1-2** | **level-2** }命令配置即可。三个多选一选项分别对应 L1 级别、L1/2 级别和 L2 级别。

缺省情况下，IS-IS 设备级别为 L1/2，即同时参与 L1 和 L2 的路由计算，维护 L1 和 L2 两个 LSDB，可用 **undo is-level** 命令用来恢复为缺省配置。在网络运行过程中，改变 IS-IS 设备的级别可能会导致 IS-IS 进程重启，并可能会造成 IS-IS 邻居断连，建议用户在配置 IS-IS 的同时完成设备级别的配置。

13.4.4 建立 IS-IS 邻居

由于 IS-IS 在广播网中和 P2P 网络中建立邻居的方式不同，因此，针对不同类型的接口，可以配置不同的 IS-IS 属性。

① 在广播网中，IS-IS 需要选择 DIS，因此通过配置 IS-IS 接口的 DIS 优先级，可以使拥有接口优先级最高的设备优选为 DIS。具体配置步骤如表 13-3 所示。

② 在 P2P 网络中，IS-IS 不需要选择 DIS，因此无需配置接口的 DIS 优先级。但是为了保证 P2P 链路的可靠性，可以配置 IS-IS 使用 P2P 接口在建立邻居时采用 3-way（也就是三次握手）模式，以检测单向链路故障。具体配置步骤如表 13-4 所示。

说明 在 P2P 网络中，通常情况下，IS-IS 会对收到的 Hello 报文进行 IP 地址检查，只有当收到的 Hello 报文的源地址和本地接收报文的接口地址在同一网段时，才会建立邻居。但当两端接口 IP 地址不在同一网段时，如果均配置了 **isis peer-ip-ignore** 命令，就会忽略对对端 IP 地址的检查，此时链路两端的 IS-IS 接口间仍可以建立正常的邻居关系。

表 13-3 广播网络中 IS-IS 邻居建立的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入要建立 IS-IS 邻居的广播类型 IS-IS 接口，进入接口视图
3	**isis enable** [*process-id*] 例如：[Huawei-GigabitEthernet1/0/0]**isis enable** 1	在接口上使能 IS-IS 功能，并指定要关联的 IS-IS 进程号，可选参数 *process-id* 用来指定要关联的 IS-IS 进程号，取值范围为 1～65 535 的整数，缺省值为 1。一个接口只能与一个 IS-IS 进程相关联 【注意】在通过 13.3.1 节全局使能 IS-IS 功能后，还必须在对应的 IS-IS 接口上使能 IS-IS 功能，否则接口仍然无法使用 IS-IS 协议。配置该命令后，IS-IS 将通过该接口建立邻居、扩散 LSP 报文 缺省情况下，接口上未使能 IS-IS 功能，可用 **undo isis enable** 命令在接口上去使能 IS-IS 功能，并取消与 IS-IS 进程号的关联

（续表）

步骤	命令	说明
4	**isis circuit-level** [**level-1** | **level-1-2** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis circuit-level level-1**	配置 IS-IS 路由器的接口链路类型，命令中的多选项说明如下 ● **level-1**：多选一可选项，指定接口链路类型为 L1，即在本接口只能建立 L1 的邻接关系 ● **level-1-2**：多选一可选项，指定接口链路类型为 L1/2，即在本接口可以同时建立 L1 和 L2 邻接关系 ● **level-2**：多选一可选项，指定接口链路类型为 L2，即在本接口只能建立 L2 邻接关系 【说明】实际上只有在接口的 IS-IS 系统类型为 L1/2 时，本命令的配置才起实质作用，否则以上节介绍的 **is-level** 命令的全局级别配置为准 在网络运行过程中，改变 IS-IS 接口的级别可能会导致网络振荡。建议用户在配置 IS-IS 时即完成路由器接口级别的配置 缺省情况下，级别为 L1/2 的 IS-IS 路由器上的接口链路类型为 L1/2，可以同时建立 L1 和 L2 的邻接关系，可用 **undo isis circuit-level** 命令恢复 L1/2 路由器的接口链路类型为缺省配置
5	**isis dis-priority** *priority* [**level-1** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis dis-priority** 127 **level-2**	（可选）设置接口在进行 DIS 选举时的优先级，命令中的参数和选项说明如下 ● *priority*：设置接口在进行 DIS 选举时的优先级，取值范围为 0～12 的整数，值越大优先级越高 ● **level-1**：二选一可选项，指定所设置的优先级为选举 L1 DIS 时的优先级 ● **level-2**：二选一可选项，指定所设置的优先级为选举 L2 DIS 时的优先级 如果不选择 Level-1 和 Level-2 可选项，则所设置的优先级同时适用于 L1 和 L2 DIS 选举 【说明】**DIS 的优先级以 Hello 报文的形式发布**。拥有最高优先级的路由器可作为 DIS。在优先级相等的情况下，拥有最高 MAC 地址的路由器被选做 DIS 缺省情况下，广播网中 IS-IS 接口在 L1 和 L2 级别的 DIS 优先级均为 64，可用 **undo isis dis-priority** [*priority*] [**level-1** | **level-2**]命令恢复缺省优先级
6	**isis silent** [**advertise-zero-cost**] 例如：[Huawei-GigabitEthernet1/0/0]**isis silent**	（可选）配置 IS-IS 接口为抑制状态，即抑制该接口接收和发送 IS-IS 报文，但此接口所在网段的直连路由仍可以通过 IS-IS 被发布出去。如果选择 advertise-zero-cost 可选项，则指定在发布直连路由时其开销值为 0，缺省情况下 IS-IS 路由的链路开销值为 10 【说明】当 IS-IS 网络与其他自治系统连接时，为了让区域内的路由器学到出口路由，需要在该出口上使能 IS-IS 协议。但这样同时会让该出接口向其所在网段发布 IS-IS Hello 报文，使其他自治系统也可以学习到 IS-IS 网络的路由。为避免 IS-IS 引入其他系统的流量，此时可以在此接口上执行本命令，启动 IS-IS 的接口抑制功能，使该接口仅使能 IS-IS 功能，但不接收和发布 IS-IS 报文 缺省情况下，不配置 IS-IS 接口为抑制状态，可用 **undo isis silent** 命令恢复为缺省状态

表 13-4 **P2P 网络中 IS-IS 邻居建立的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入要 P2P 邻居的 P2P IS-IS 接口，进入接口视图
3	**isis enable** [*process-id*] 例如：[Huawei-GigabitEthernet1/0/0]**isis enable** 1	在接口上使能 IS-IS 功能并指定要关联的 IS-IS 进程号，其他说明参见表 13-3 中的第 3 步
4	**isis circuit-level** [**level-1** | **level-1-2** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis circuit-level level-1**	配置 IS-IS 路由器的接口链路类型，其他说明参见表 13-3 中的第 4 步
5	**isis circuit-type p2p** 例如：[Huawei-GigabitEthernet1/0/0] **isis circuit-type p2p**	（可选）将 IS-IS 广播网接口的网络类型模拟为 P2P 类型。由于 IS-IS 在广播网中和 P2P 网络中建立邻居的方式不同，因此在网络中链路两端的 IS-IS 接口的网络类型必须一致，否则双方不可以建立起邻居关系。一般来说，广播网中接口的网络类型都是以太类型，而封装 PPP、HDLC 等协议的链路接口的网络类型都是 P2P 类型。可通过执行本命令实现将广播类型的 IS-IS 接口模拟为 P2P 类型，从而实现网络类型达到一致，保证邻居关系的正常建立 缺省情况下，接口网络类型根据物理接口决定，可用 **undo isis circuit-type** 命令恢复 IS-IS 接口的缺省网络类型 【说明】在使能 IS-IS 的接口上，当接口类型发生改变时，相关配置发生改变，具体如下： • 使用本命令将广播网接口模拟成 P2P 接口时，接口发送 Hello 报文的间隔时间、宣告邻居失效前 IS-IS 没有收到的邻居 Hello 报文数目、点到点链路上 LSP 报文的重传间隔时间以及 IS-IS 各种验证均恢复为缺省配置，而 DIS 优先级、DIS 名称、广播网络上发送 CSNP 报文的间隔时间等配置均失效 • 使用 **undo isis circuit-type** 命令恢复接口的网络类型时，接口发送 Hello 报文的间隔时间、宣告邻居失效前 IS-IS 没有收到的邻居 Hello 报文数目、点到点链路上 LSP 报文的重传间隔时间、IS-IS 各种验证、DIS 优先级和广播网络上发送 CSNP 报文的间隔时间均恢复为缺省配置
6	**isis ppp-negotiation** { **2-way** | **3-way** [**only**] } 例如：[Huawei-GigabitEthernet1/0/0] **isis ppp-negotiation 2-way**	（可选）指定在建立邻接关系时采用的 PPP 协商类型。命令中的选项说明如下： • **2-way**：二选一选项，指定建立邻接关系时使用二次握手（2-Way Handshake）的协商模型 • **3-way**：二选一选项，指定建立邻接关系时使用三次握手（3-Way Handshake）的协商模型。三次握手模型为后向兼容，如果对方只支持二次握手，则建立二次握手模型下的邻接关系 • **only**：可选项，指定建立邻接关系时只使用三次握手的协商模型，不支持后向兼容 **本命令只适用于点到点链路接口，对于广播接口，需在接口上配置链路类型为 P2P 后才可使用** 缺省情况下，采用三次握手协商模型，可用 **undo isis ppp-negotiation** 命令恢复协商模式为缺省模式

（续表）

步骤	命令	说明
7	**isis peer-ip-ignore** 例如：[Huawei-GigabitEthernet1/0/0] **isis peer-ip-ignore**	（可选）配置对接收的 Hello 报文不作 IP 地址检查 【说明】通常情况下，IS-IS 会对收到的 Hello 报文进行 IP 地址检查，只有这个地址和本地接收报文的接口地址在同一网段时，才会建立邻居。但如果两端接口 IP 地址不在同一网段，均配置了 **isis peer-ip-ignore** 命令，就会忽略对对端 IP 地址的检查，此时链路两端的 IS-IS 接口间可以建立正常的邻居关系。路由表中有这两个不同网段的路由，但是不能互相 Ping 通 缺省情况下，IS-IS 检查对端 Hello 报文的 IP 地址，可用 **undo isis peer-ip-ignore** 命令恢复为缺省状态
8	**isis ppp-osicp-check** 例如：[Huawei-GigabitEthernet1/0/0] **isis ppp-osicp-check**	（可选）配置 PPP 链路协议的接口检查 OSICP（开放系统互联控制协议，相当于 TCP/IP 网络中的 TCP）协商状态，协商状态会影响接口在 IS-IS 下的状态。**本命令仅适用于 OSI 网络** 缺省情况下，IS-IS 忽略 PPP 协议的 OSICP 状态，可用 **undo isis ppp-osicp-check** 命令恢复为缺省情况

13.4.5　配置 IS-IS 主机名映射

通常在运行 IS-IS 协议的设备上，查看 IS-IS 邻居和链路状态数据库等信息时，IS-IS 域中的各设备都是用由 12 位十六进制数组成的 System ID 来表示的，例如：aaaa.eeee.1234。这种表示方法比较繁琐，而且易用性不好。为方便对 IS-IS 网络进行维护和管理，IS-IS 协议引入了动态和静态主机名映射机制。配置 IS-IS 主机名映射后，在使用 **display** 命令查看 IS-IS 的相关信息时，会以配置的动态名称代替设备的 System ID，从而提高 IS-IS 网络的可维护性。

在下列三种情况下会将 System ID 替换为主机名显示。

① 显示 IS-IS 邻居时，将 IS-IS 邻居的 System ID 替换为主机名。如果该邻居为 DIS，则 DIS 的 System ID 也替换为该邻居的主机名。

② 显示 IS-IS 链路状态数据库中的 LSP 时，将 LSP ID 中的 System ID 替换为发布该 LSP 的设备的主机名。

③ 显示 IS-IS LSDB 的详细信息时，对于使能了动态主机名交换的设备发送的 LSP 报文会增加显示 Host Name 字段，而此字段显示内容中的 System ID 也将替换为发送此 LSP 的设备的动态主机名。

IS-IS 主机名映射机制包括动态主机名映射和静态主机名映射。动态主机名映射的优先级高于静态主机名映射。当两者同时存在时，由动态主机名代替静态主机名。

1. 配置动态主机名映射

在使能了动态主机名映射的设备上，IS-IS 动态主机名的信息在 LSP 中以 137 号 TLV（Dynamic Hostname TLV）的形式发布给其他 IS-IS 设备。在其他设备上使用 IS-IS 相关显示命令查看 IS-IS 信息时，本地设备的 System ID 将被设置的主机名所代替，这样更直观，也更容易记忆。但动态主机名的 TLV 是可选的，且可以存在于 LSP 中的任何位置，

其中的 value 值不能为空。设备在发送 LSP 的时候可以决定是否携带该 TLV，接收端的设备也可以决定是否忽略该 TLV，或者提取该 TLV 的内容放在自己的映射表中。

配置动态主机名映射的方法很简单，是在 IS-IS 进程下使用 **is-name** *symbolic-name* 命令进行的，使能识别 LSP 报文中主机名称的能力，**同时为本地路由器上 IS-IS 系统配置动态主机名**，并以 LSP 报文的方式发布出去。参数 *symbolic-name* 用来指定动态主机名，1～64 个字符，区分大小写，不支持空格。该配置属于动态配置，即配置的主机名称 *symbolic-name* 以 LSP 报文的形式发布给区域中的其他 IS-IS 设备。在其他设备上使用 IS-IS 相关显示命令查看 IS-IS 信息时，系统 ID 将被 *symbolic-name* 代替。配置成功后，可以通过 **display isis name-table** 命令查看到所配置的主机名称。

缺省情况下，本地路由器上的 IS-IS 系统没有动态主机名，可用 **undo is-name** [*symbolic-name*]命令删除本地路由器上所有或者指定的 IS-IS 系统的动态主机名。

【示例】为本地 IS-IS 系统配置名称为 RUTA。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] is-name RUTA
```

2. 配置静态主机名映射

配置静态主机名映射的方法也很简单，是在 IS-IS 进程下执行 **is-name map** *system-id symbolic-name* 命令，使能本地路由器识别 LSP 报文中主机名称的功能，并在本端**为远端 IS-IS 路由器配置一个静态主机名**。该配置属于静态配置，**仅对本地设备生效**，配置的主机名称 *symbolic-name* 不会通过 LSP 报文发送出去。因此，如果网络中的对应的 IS-IS 设备配置了动态主机名映射，那么该映射关系将覆盖本地设备的静态映射。命令中的参数说明如下。

① *system-id*：指定远端被映射 IS-IS 系统 ID 或伪节点 ID，格式为 XXXX.XXXX.XXXX[.XX]，X 为十六进制数。

② *symbolic-name*：指定远端被映射 IS-IS 系统的静态主机名，1～64 个字符，区分大小写，不支持空格。

使用此命令为远端设备和主机名建立映射关系后，可使用 **display isis name-table** 命令查看信息时，此时远端设备的系统 ID 会被设置的主机名代替。

缺省情况下，未使能本地路由器识别 LSP 报文中主机名称的功能，且本端没有为远端 IS-IS 系统配置静态主机名，可用 **undo is-name map** *system-id* [*symbolic-name*]命令去使能本地路由器识别 LSP 报文中主机名称的功能，并删除本端为远端 IS-IS 系统配置的指定或所有系统 ID 映射的静态主机名。

【示例】为远端路由器的 IS-IS 系统（0000.0000.0041）配置静态名称 RUTB 映射。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] is-name map 0000.0000.0041 RUTB
```

13.4.6 IS-IS 基本功能管理

配置好 IS-IS 基本功能后，可通过以下 **display** 视图命令查看相关信息，验证配置结果，也可使用以下 **reset** 用户视图命令复位 IS-IS 数据结构或者邻居关系。

① **display isis peer** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]：查看指定或所有 IS-IS 进程中的邻居信息。

② **display isis interface** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]：查看指定或所有 IS-IS 进程中使能了 IS-IS 的接口信息。

③ **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* |*mask-length*]] *：查看指定或所有 IS-IS 进程中的 IS-IS 的路由信息。

④ **display isis** *process-id* **lsdb** [[**level-1** | **level-2**] | **verbose** | [**local** | *lsp-id* | **is-name** *symbolic-name*]] *查看指定进程下符合条件的 IS-IS 的链路状态数据库信息。

⑤ **display isis name-table**：查看本地和远端 IS-IS 设备主机名到系统 ID 的映射关系表。

⑥ **reset isis all** [[*process-id* | **vpn-instance** *vpn-instance-name*] | **graceful-restart**] *：复位指定或所有 IS-IS 进程的数据结构。

⑦ **reset isis peer** *system-id* [*process-id* | **vpn-instance** *vpn-instance-name*]：复位指定或所有 IS-IS 进程的特定邻居。**当 IS-IS 路由策略或协议发生变化后，需要通过复位 IS-IS 特定邻居使新的配置生效。**

13.4.7　IS-IS 基本功能配置示例

本示例的基本拓扑结构如图 13-21 所示，现网中有 4 台路由器。用户希望利用这 4 台路由器通过 IS-IS 协议实现网络互联，并且因为 RouterA 和 RouterB 性能相对较低，所以还要使这两台路由器处理的数据信息相对较少。

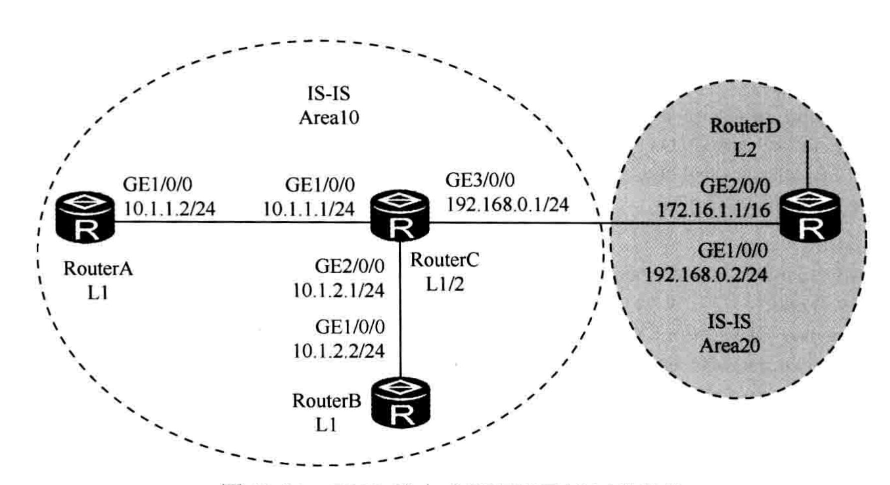


图 13-21　IS-IS 基本功能配置示例拓扑结构

1. 基本配置思路分析

本示例通过配置基本的 IS-IS 功能就可以实现各路由器网络的互通了。但要特别注意的是，示例中要求 RouterA 和 RouterB 仅需处理较少的数据，就需要把它们配置成普通区域中的 L1 路由器，在一定程度上类似于 OSPF 中的 Stub 区域中的内部路由器。当然首先还得配置各路由器接口的 IP 地址，使它们之间三层可达。

根据本示例的拓扑结构可以得出，这时同时与 RouterA 和 RouterB 相连的 RouterC

成了 L1/2 路由器，相当于 OSPF 中的区域边界路由器。而一个 IS-IS 网络中，至少得有一个骨干区域，所以 RouterD 自然就需要单独划分为骨干区域，为 L2 路由器。但它不可能与 RouterA 和 RouterB 同处一个区域，因为 RouterA 和 RouterB 已确定是位于普通区域中的。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 为例进行介绍，RouterB、RouterC 和 RouterD 的配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.2 24
```

② 配置各路由器的 IS-IS 基本功能，包括启动 IS-IS 进程（同样进程号只对本地设备有意义），配置全局路由器级别、网络实体名称，并要在各 IS-IS 接口上使能 IS-IS 功能。这里为了方便区分和记忆，把这 4 台路由器的 System ID 分别配置为 0000.0000.0001、0000.0000.0002、0000.0000.0003、0000.0000.0004（每个必须是 12 位十六进制数）。

RouterA 上的配置如下。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
```

RouterC 上的配置如下。

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable 1
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] isis enable 1
[RouterC-GigabitEthernet3/0/0] quit
```

RouterD 上的配置如下。

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] isis enable 1
```

```
[RouterD-GigabitEthernet2/0/0] quit
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis enable 1
[RouterD-GigabitEthernet1/0/0] quit
```

配置好后，可以在各路由器上执行 **display isis lsdb** 命令显示 IS-IS LSDB 信息，查看它们的 LSDB 是否同步，验证配置结果。其中"*(In TLV)"表示渗透路由，"*(By LSPID)"表示本地生成的 LSP，"+"表示本地生成的扩展 LSP。在 L1 路由器中有 L1 LSDB，在 L1/2 路由器中同时有 L1 LSDB 和 L2 LSDB，在 L2 路由器只有 L2 LSDB。从中可以看，同处于区域 10 的 RouterA、RouterB 和 RouterC 的 L1 LSDB 是完全一样的，实现了同步；而同位于 L2 区域的 RouterC 和 RouterD 的 L2 LSDB 也是完全一样的，也实现了同步。

```
[RouterA] display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                  Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------
0000.0000.0001.00-00* 0x00000006   0xbf7d        649           68      0/0/0
0000.0000.0002.00-00  0x00000003   0xef4d        545           68      0/0/0
0000.0000.0003.00-00  0x00000008   0x3340        582           111     1/0/0
Total LSP(s): 3
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload

[RouterB] display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                  Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xbf7d        642           68      0/0/0
0000.0000.0002.00-00* 0x00000003   0xef4d        538           68      0/0/0
0000.0000.0003.00-00  0x00000008   0x3340        574           111     1/0/0
Total LSP(s): 3
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload

[RouterC] display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                  Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xbf7d        638           68      0/0/0
0000.0000.0002.00-00  0x00000003   0xef4d        533           68      0/0/0
```

```
0000.0000.0003.00-00* 0x00000008   0x3340      569         111      1/0/0
Total LSP(s): 3

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload

                          Level-2 Link State Database

LSPID                  Seq Num      Checksum      Holdtime      Length   ATT/P/OL
-------------------------------------------------------------------------
0000.0000.0003.00-00* 0x00000008   0x55bb      650         100      0/0/0
0000.0000.0004.00-00  0x00000005   0x6510      629         84       0/0/0
Total LSP(s): 2
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload

[RouterD] display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-2 Link State Database

LSPID                  Seq Num      Checksum      Holdtime      Length   ATT/P/OL
-------------------------------------------------------------------------
0000.0000.0003.00-00  0x00000008   0x55bb      644         100      0/0/0
0000.0000.0004.00-00* 0x00000005   0x6510      624         84       0/0/0
Total LSP(s): 2
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload
```

还可通过 **display isis route** 命令显示各路由器的 IS-IS 路由信息。L1 路由器的路由表中应该有一条缺省路由，且下一跳为 L1/2 路由器，L2 路由器应该有所有 L1 和 L2 的路由（**参见输出信息中的粗体字部分**）。输出信息中的“IntCost”为 IS-IS 路由的开销值，“ExtCost”为由外部引入的其他协议路由的开销值，“ExitInterface”为路由的出接口，“NextHop”为路由的下一跳地址。当目的网段为设备直连网段时，显示为 Direct，“Flags”为路由信息标记，不同路由的标记具体如下。

① D：表示直连路由。

② A：表示此路由被加入单播路由表中。

③ L：表示此路由通过 LSP 发布出去。

```
[RouterA] display isis route

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

IPV4 Destination    IntCost    ExtCost ExitInterface    NextHop          Flags
-------------------------------------------------------------------------
10.1.1.0/24         10         NULL     GE1/0/0          Direct          D/-/L/-
10.1.2.0/24         20         NULL     GE1/0/0          10.1.1.1        A/-/-/-
```

```
192.168.0.0/24      20        NULL      GE1/0/0          10.1.1.1        A/-/-/-
0.0.0.0/0           10        NULL      GE1/0/0          10.1.1.1        A/-/-/-

      Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set

[RouterB] display isis route

                         Route information for ISIS(1)
                         -----------------------------

                         ISIS(1) Level-1 Forwarding Table
                         --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface     NextHop          Flags
------------------------------------------------------------------------
 10.1.2.0/24          10         NULL      GE1/0/0          Direct          D/-/L/-
 10.1.1.0/24          20         NULL      GE1/0/0          10.1.2.1        A/-/-/-
 192.168.0.0/24       20         NULL      GE1/0/0          10.1.2.1        A/-/-/-
 0.0.0.0/0            10         NULL      GE1/0/0          10.1.2.1        A/-/-/-

      Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set

[RouterC] display isis route

                         Route information for ISIS(1)
                         -----------------------------

                         ISIS(1) Level-1 Forwarding Table
                         --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface     NextHop          Flags
------------------------------------------------------------------------
 10.1.1.0/24          10         NULL      GE1/0/0          Direct          D/-/L/-
 10.1.2.0/24          10         NULL      GE2/0/0          Direct          D/-/L/-
 192.168.0.0/24       10         NULL      GE3/0/0          Direct          D/-/L/-
      Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set


                         ISIS(1) Level-2 Forwarding Table
                         --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface     NextHop          Flags
------------------------------------------------------------------------
 10.1.1.0/24          10         NULL      GE1/0/0          Direct          D/-/L/-
 10.1.2.0/24          10         NULL      GE2/0/0          Direct          D/-/L/-
 192.168.0.0/24       10         NULL      GE3/0/0          Direct          D/-/L/-
 172.16.0.0/16        20         NULL      GE3/0/0          192.168.0.2     A/-/-/-

      Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                              U-Up/Down Bit Set
```

```
[RouterD] display isis route

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------
 IPV4 Destination     IntCost    ExtCost ExitInterface     NextHop         Flags
------------------------------------------------------------------------------
 192.168.0.0/24       10         NULL     GE3/0/0           Direct          D/-/L/-
 10.1.1.0/24          20         NULL     GE3/0/0           192.168.0.1     A/-/-/-
 10.1.2.0/24          20         NULL     GE3/0/0           192.168.0.1     A/-/-/-
 172.16.0.0/16        10         NULL     GE2/0/0           Direct          D/-/L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                            U-Up/Down Bit Set
```

13.5 IS-IS 路由聚合

在部署 IS-IS 的大规模网络中，路由条目过多，会导致在转发数据时降低路由表查找速度，同时会增加管理复杂度。通过配置路由聚合，可以减小路由表的规模。同时，如果被聚合的 IP 地址范围内的某条链路频繁 Up 和 Down，该变化不会通告到被聚合的 IP 地址范围外的设备。因此，可以避免网络中的路由振荡，提高了网络的稳定性。

13.5.1 配置 IS-IS 路由聚合

IS-IS 的路由聚合是在 IS-IS L1/2 路由器上配置的，就是为了减少所连区域内 L1 路由器，或者所引入的其他协议路由器向区域外通告的路由数量，使区域外路由器可以通过一条聚合路由与区域内 L1 路由器进行通信。要注意的是，**路由器只对本地生成，并向 IS-IS 邻居路由器发布的 LSP 中的路由进行聚合，不对从邻居 IS-IS 路由器接收的 LSP 中的路由进行聚合**。即配置路由聚合后不会影响 L1 和 L1/2 路由器上本地设备的路由表，仍然会显示每一条具体路由，只是会减少通过 L1/2 路由器向区域外部扩展的 LSP 报文数。

被聚合的路由可以是 IS-IS 路由，也可以是被引入的其他协议路由。聚合后路由的开销值取所有被聚合路由中学习到的路由的最小开销值。在 IS-IS 路由聚合的具体配置过程中，在对应的 IS-IS 进程下使用 **summary** *ip-address mask* [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] * 命令进行设置。在配置 IS-IS 路由聚合之前，需配置 IS-IS 的基本功能。命令中的参数和选项说明如下。

① *ip-address mask*：指定聚合路由的网络 IP 地址和子网掩码。IS-IS 聚合路由的子网掩码前缀长度也必须小于所有被聚合路由的子网掩码长度，可以是对应的自然网段路由，甚至超网路由。

② **avoid-feedback**：可多选选项，为避免本地路由器通过路由 SPF 计算再次学习到这条聚合路由。因为聚合路由主要是向外发布的，不需要在本地路由表中存在。

③ **generate_null0_route**：可多选选项，为防止路由环路，在本地路由器上为配置的聚合路由生成一条下一跳为 Null 0 的黑洞路由。

④ **tag** *tag*：可多选选项，表示为发布的聚合路由分配管理标记，取值范围为 1～4 294 967 295 的整数。

⑤ **level-1**：多选一可选项，表示只对引入到本地路由器 L1 区域的路由进行聚合。如果没有指定 Level 级别，缺省为 L2。

⑥ **level-1-2**：多选一可选项，表示对引入到本地路由器的 L1 区域和 L2 区域的路由都进行聚合。如果没有指定 Level 级别，缺省为 L2。

⑦ **level-2**：多选一可选项，表示只对引入到本地路由器的 L2 区域的路由进行聚合。如果没有指定 Level 级别，缺省为 L2。

缺省情况下，没有配置 IS-IS 生成聚合路由，可用 **undo summary** *ip-address mask* [**level-1** | **level-1-2** | **level-2**]命令取消 IS-IS 生成的指定聚合路由。

【示例】在一个 L1/2 路由器中配置一条 202.0.0.0/8 的 IS-IS 聚合路由。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] summary 202.0.0.0 255.0.0.0
```

在 L1/2 路由器上配置好聚合路由后，可在网络中的其他路由器上通过执行 **display isis route** 命令查看 IS-IS 路由表中的聚合路由；可在网络中的其他路由器上通过执行 **display ip routing-table** [**verbose**]命令查看 IP 路由表中的聚合路由。

13.5.2　IS-IS 路由聚合配置示例

本示例的基本拓扑结构如图 13-22 所示，网络中有 3 台路由器通过 IS-IS 路由协议实现互联，且 RouterA 为 L2 路由器，RouterB 为 L1/2 路由器，RouterC 为 L1 路由器。但是由于 IS-IS 网络的路由条目过多造成 RouterA 系统资源负载过重，现要求降低 RouterA 的系统资源的消耗。

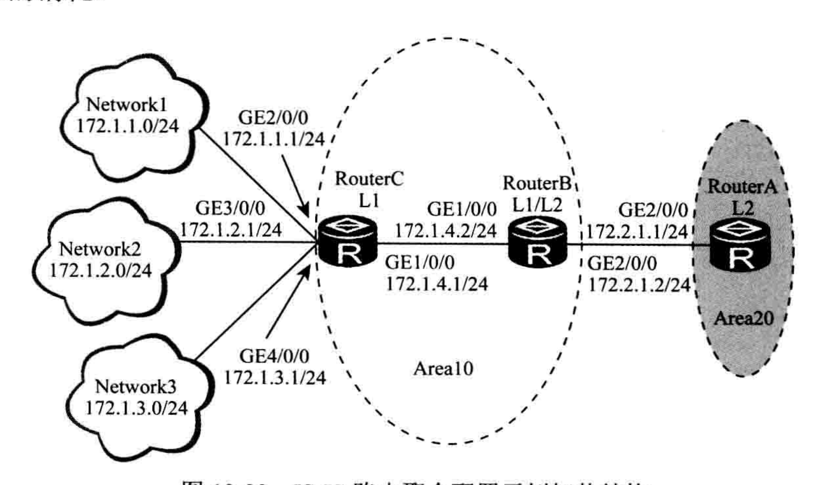


图 13-22　IS-IS 路由聚合配置示例拓扑结构

1. 基本配置思路分析

本示例主要需要完成以下配置任务。

① 配置各路由器的接口 IP 地址，以便它们之间三层可达。

② 在各路由器上配置基本的 IS-IS 功能，实现网络互联。

③ 在 RouterB 上配置路由聚合，对所连接的 Network1（172.1.1.0/24）、Network2（172.1.2.0/24）和 Network3（172.1.3.0/24）以及 172.1.4.0/24 这 4 个连续子网的路由在 RouterB 上以一条聚合路由向 RouterA 发布，使得在不影响数据转发的前提下减少 RouterA 中路由表规模，从而降低 RouterA 系统资源的消耗。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。现仅以 RouterA 上的配置为例进行介绍，RouterB 和 RouterC 的配置方法一样，略。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 172.2.1.1 24
```

② 在各路由器上配置 IS-IS 基本功能，包括全局使能 IS-IS 功能、配置网络实体名称、在各接口上但使能 IS-IS 功能。在网络实体名称配置中，RouterA、RouterB 和 RouterC 的系统 ID 分别设为 0000.0000.0001、0000.0000.0002 和 0000.0000.0003（均为 12 位十六进制）。

RouterA 上的配置如下。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-2
[RouterA-isis-1] network-entity 20.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis enable 1
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
```

RouterC 上的配置如下。

```
[RouterC] isis 1
[RouterC-isis-1] is-level level-1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable 1
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] isis enable 1
[RouterC-GigabitEthernet3/0/0] quit
[RouterC] interface gigabitethernet 4/0/0
```

```
[RouterC-GigabitEthernet4/0/0] isis enable 1
[RouterC-GigabitEthernet4/0/0] quit
```

配置好后，可以在 RouterA 上通过 **display isis route** 命令查看 IS-IS 路由表信息。从中可以看出，在 RouterA 上面有到达 RouterC 上连接的 4 个连续子网的 IS-IS 路由表项（**参见输出信息中的粗体字部分**）。

```
[RouterA] display isis route
                         Route information for ISIS(1)
                         -----------------------------
                         ISIS(1) Level-2 Forwarding Table
                         --------------------------------
 IPV4 Destination    IntCost    ExtCost    ExitInterface     NextHop       Flags
-------------------------------------------------------------------------------
 172.1.1.0/24        30         NULL       GE2/0/0           172.2.1.2     A/-/L/-
 172.1.2.0/24        30         NULL       GE2/0/0           172.2.1.2     A/-/L/-
 172.1.3.0/24        30         NULL       GE2/0/0           172.2.1.2     A/-/L/-
 172.1.4.0/24        20         NULL       GE2/0/0           172.2.1.2     A/-/L/-
 172.2.1.0/24        10         NULL       GE2/0/0           Direct        D/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                                U-Up/Down Bit Set
```

③ 在 RouterB 上配置路由聚合，将 172.1.1.0/24、172.1.2.0/24、172.1.3.0/24、172.1.4.0/24 这 4 个连续子网的路由聚合成 172.1.0.0/16。这里要注意的是，因为这 4 个子网都属于 L1 区域，所以仅需对引入 L1 区域中的路由进行聚合。

```
[RouterB] isis 1
[RouterB-isis-1] summary 172.1.0.0 255.255.0.0 level-1
[RouterB-isis-1] quit
```

现在再来通过 **display isis route** 命令查看 RouterA 的路由表，验证配置结果。从中可以看到 172.1.1.0/24、172.1.2.0/24、172.1.3.0/24 和 172.1.4.0/24 聚合成了 172.1.0.0/16 一条路由（**参见输出信息中的粗体字部分**）。

```
[RouterA] display isis route
                         Route information for ISIS(1)
                         -----------------------------
                         ISIS(1) Level-2 Forwarding Table
                         --------------------------------
 IPV4 Destination    IntCost    ExtCost ExitInterface    NextHop          Flags
-------------------------------------------------------------------------------
 172.1.0.0/16        20         NULL       GE2/0/0           172.2.1.2     A/-/L/-
 172.2.1.0/24        10         NULL       GE2/0/0           Direct        D/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                                U-Up/Down Bit Set
```

13.6　控制 IS-IS 的路由信息交互

在网络中同时部署了 IS-IS 和其他路由协议时，需要配置 IS-IS 与其他路由协议的路由交互，才能使运行不同协议的网络正常通信。控制 IS-IS 的路由信息交互所涉及的配置任务如下（它们是并列关系，根据实际需要选择一项或多项进行配置）。

① 配置 IS-IS 发布缺省路由。

② 配置 IS-IS 引入外部路由。

③ 配置 IS-IS 发布外部路由过滤。

④ 配置 IS-IS 路由下发 IP 路由表过滤。

在配置控制 IS-IS 的路由信息的交互之前，也需要配置 IS-IS 的基本功能。

13.6.1 配置 IS-IS 发布缺省路由

通常，当网络中部署了 IS-IS 和其他路由协议时，为了实现 IS-IS 域内的流量可以到达 IS-IS 域外，通常有如下两种方式。

① **在边界设备上**配置 IS-IS 设备向 IS-IS 域发布缺省路由。

② **在边界设备上**将其他路由域的路由引入 IS-IS 中。

其中，配置发布缺省路由的方式较为简单，不需要学习外部路由。在具有外部路由的边界设备上配置 IS-IS 发布缺省路由可以使该设备在 IS-IS 路由域内发布一条 0.0.0.0/0 的缺省路由，这样，IS-IS 域内的其他设备在转发流量时，将所有去往外部路由域的流量首先通过这条缺省路由转发到该设备，然后通过该设备去往外部路由域。

说明 虽然配置静态缺省路由也可以实现以上功能，但是当现网中有大量设备时，配置工作量巨大，且不利于管理。另外，采用 IS-IS 发布缺省路由的方式更加灵活。例如，如果存在多个边界设备，那么可以通过配置路由策略，使某台边界设备在满足条件时才发布缺省路由，从而避免造成路由黑洞。**有关路由策略的详细介绍和配置方法参见第 15 章。**

IS-IS 发布缺省路由的方法是在 IS-IS 进程下执行 **default-route-advertise** [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost* | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] * [**avoid-learning**]命令。命令中的参数和选项说明如下。

① **always**：多选一选项，指定设备无条件地发布缺省路由，且发布的缺省路由中将自己作为下一跳。

② **match default**：多选一选项，指定如果在路由表中存在其他路由协议或其他 IS-IS 进程生成的缺省路由，则在 LSP 中发布该缺省路由。

③ **route-policy** *route-policy-name*：多选一参数，指定当该边界设备的路由表中存在满足指定名称（1～40 个字符，区分大小写，不支持空格）路由策略的外部路由时，才向 IS-IS 域发布缺省路由，避免由于链路故障等原因造成该设备已经不存在某些重要的外部路由时，仍然发布缺省路由从而造成路由黑洞。此处的路由策略不影响 IS-IS 引入外部路由。

④ **cost** *cost*：可多选参数，指定缺省路由的开销值，取值范围要根据 cost-style 而定。当 cost-style 为 narrow、narrow-compatible 或 compatible 时，取值范围为 0～63 的整数；当 cost-style 为 wide 或 wide-compatible 时，取值范围为 0～4 261 412 864 的整数。

⑤ **tag** *tag*：可多选参数，指定发布的缺省路由的标记值。只有当 IS-IS 的开销类型为 wide、wide-compatible 或 compatible 时，发布的 LSP 中才会携带 tag 值。

⑥ **level-1** | **level-1-2** | **level-2**：可多选选项，分别指定发布的缺省路由级别为 L1、L1/2、L2。如果不指定级别，则默认为生成 L2 级别的缺省路由。

⑦ **avoid-learning**：可选项，指定避免 IS-IS 进程学到其他路由协议或其他 IS-IS 进

程生成的缺省路由并添加到路由表。如果路由表中已存在学习到的缺省路由为活跃状态，则将此路由置为不活跃状态。

如果在 L1 设备上配置了该命令，那么该设备只会向 L1 区域发布缺省路由，不会将缺省路由发布到 L2 区域。

缺省情况下，运行 IS-IS 协议的设备不生成缺省路由，可用 **undo default-route-advertise** 命令取消运行 IS-IS 协议的设备生成缺省路由。

【示例】设置当前设备发布匹配名为 **filter** 的路由策略的 IPv4 缺省路由，并设置该缺省路由的开销值为 15。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] default-route-advertise route-policy filter cost 15
```

13.6.2 配置 IS-IS 引入外部路由

按照上节介绍的方法，**在 IS-IS 路由域边界设备**上配置 IS-IS 发布缺省路由，可以将去往 IS-IS 路由域外部的流量全部转到该设备来处理，这样一来就可能会造成该边界设备的负担过重。此外，在有多个边界设备时，会存在去往其他路由域的最优路由的选择问题。此时，通过在边界设备上引入外部路由，让 IS-IS 域内的其他设备获悉全部或部分外部路由的方法就可以解决以上两个问题。

引入的外部路由包括其他进程 IS-IS 路由、静态路由、直连路由、RIP 路由、OSPF 路由和 BGP 路由等。配置引入外部路由后，IS-IS 设备将把引入的外部路由全部发布到 IS-IS 路由域。在这里有两种不同的配置方式。

① 当需要对引入路由的开销进行设置时，可在对应 IS-IS 进程下通过 **import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **static** | **direct** | **unr** | **bgp** [**permit-ibgp**] } [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * 命令配置。

② 当需要保留引入路由的原有开销时，可在对应 IS-IS 进程下通过 **import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **unr** | **bgp** }**inherit-cost** [**tag** *tag* | **route- policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * 命令配置 IS-IS 引入外部路由。但此时引入的源路由协议不能是 **static**（静态路由）。

以上两个命令中的参数和选项说明如下。

① **rip**：多选一选项，引入 RIP 路由。

② **isis**：多选一选项，引入其他进程 IS-IS 路由。

③ **ospf**：多选一选项，引入 OSPF 路由。

④ *process-id*：可选参数，指定引入的 RIP，或者 IS-IS，或者 OSPF 路由的进程号，取值范围为 1～65 535 的整数。指定此参数时，缺省值为 1。

⑤ **static**：多选一选项，指定引入静态路由。

⑥ **direct**：多选一选项，指定引入直连路由。

⑦ **unr**：多选一选项，指定引入用户网络路由。

⑧ **bgp**：多选一选项，指定引入 BGP 路由。

⑨ **permit-ibgp**：可选项，指定在引入 iBGP 路由时，不指定此可选项时，则引入的

为 eBGP 路由。

⑩ **cost-type** {**external** |**internal** }：可多选选项，指定引入外部路由的开销类型。缺省情况下为 **external**。此参数的配置会影响引入路由的 cost 值：当引入的路由开销类型配置为 **external** 时，路由 cost 值=源路由 cost 值+64；当引入的路由开销类型配置为 **internal** 时，路由 cost 值继承源路由的 cost 值。当路由器的 cost-style 为 wide、compatible 或 wide-compatible 时，引入外部路由的开销类型将不区分 **external** 和 **internal**。

⑪ **cost** *cost*：可多选参数，指定引入后的路由开销值，当路由器的 cost-style 为 wide 或 wide-compatible 时，引入路由的开销值取值范围是 0～4 261 412 864，否则取值范围是 0～63。缺省值是 0。

⑫ **inherit-cost**：表示引入外部路由时保留路由的原有开销值，这时将不能配置引入路由的开销类型和开销值。

⑬ **tag** *tag*：可多选参数，指定引入后的路由标记，取值范围为 1～4 294 967 295 的整数。

⑭ **route-policy** *route-policy-name*：可多选参数，指定用于限制外部路由引入的路由策略名称，命名规则包括 1～40 个字符、区分大小写、不支持空格。

⑮ **level-1**：多选一选项，表示引入路由到 L1 的路由表中。如果不指定级别，默认为引入路由到 L2 路由表中。

⑯ **level-2**：多选一选项，表示引入路由到 L2 的路由表中。如果不指定级别，默认为引入路由到 L2 路由表中。

⑰ **level-1-2**：多选一选项，表示引入路由同时到 L1 和 L2 的路由表中。如果不指定级别，默认为引入路由到 L2 路由表中。

尽管以上参数和选项非常多，但其中绝大多数是可选参数和可选项，都有缺省值，所以一般情况下，在配置路由引入时仅需指定必须的少数几个参数和选项。

缺省情况下，IS-IS 不引入其他路由协议的路由信息，以上两个配置命令可分别用 **undo import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **static** | **direct** | **unr** | **bgp** [**permit-ibgp**] } [**cost-type** { **external** |**internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *、**undo import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **unr** | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy***route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *命令删除指定的路由引入配置。

【示例 1】配置 IS-IS 引入静态路由，并设置该路由的开销值为 15。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] import-route static cost 15
```

【示例 2】配置 IS-IS 引入 OSPF 路由，并保留该路由的原有开销值。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] import-route ospf inherit-cost
```

13.6.3 配置 IS-IS 发布外部路由过滤

当 IS-IS 路由域边界路由器将引入的外部路由发布给其他 IS-IS 设备时，如果对方 IS-IS 设备不需要拥有全部的外部路由，则可以通过配置基本 ACL 或 IP 地址前缀列表或

路由策略来控制只发布部分外部路由给其他 IS-IS 设备。

IS-IS 发布外部路由过滤的配置方法是在对应的 IS-IS 进程下执行 **filter- policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }**export** [*protocol* [*process-id*]]命令并配置。其中的参数说明如下。

① *acl-number*：多选一参数，指定用于过滤外部路由发布的 ACL 列表号，取值范围 2 000～2 999 的整数，即仅可以是基本 ACL，用于过滤路由中的目的 IP 地址。

② **acl-name** *acl-name*：多选一参数，指定用于过滤外部路由发布的 ACL 名称，1～32 个字符，区分大小写，不支持空格。只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对过滤规则有效。

③ **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤外部路由发布的 IP 地址前缀列表名称，1～169 个字符，区分大小写，不支持空格。

④ **route-policy** *route-policy-name*：多选一参数，指定用于过滤外部路由发布的路由策略名称，1～40 个字符，区分大小写，不支持空格。

⑤ *protocol*：可选参数，指定哪些已引入的路由信息在发布时要进行过滤，取值包括 **direct**、**static**、**rip**、**bgp**、**unr**、**ospf** 以及其他 isis 进程。如果省略该参数，将对所有发布的外部路由都进行过滤。

⑥ *process-id*：可选参数，当要进行发布过滤的外部路由是 **rip**、**ospf** 或其他 **isis** 进程路由时，指定对应外部路由的进程号，取值范围为 1～65 535 的整数。如果不指定本参数，则进程号为缺省值 1。

说明 配置该命令后，不会影响引入的外部路由添加到本地设备的路由表中，只会对 IS-IS 邻居设备发布的外部路由进行过滤。

【示例】配置 IS-IS 使用编号为 2000 的 ACL，仅允许已引入的外部路由 1.1.1.0/24 在发布给其他路由器时进行过滤。

```
<Huawei> system-view
[Huawei]acl 2000
[Huawei-acl-basic-2000]rule permit source 1.1.1.0 0.255.255.255
[Huawei] isis
[Huawei-isis-1] filter-policy 2000 export
```

13.6.4　配置 IS-IS 路由下发 IP 路由表过滤

IP 报文是根据 IP 路由表来进行转发的。IS-IS 路由表中的路由条目需要被成功下发到 IP 路由表中，该路由条目才生效。因此，可以通过配置基本 ACL、IP 地址前缀列表、路由策略等方式，只允许匹配的 IS-IS 路由下发到 IP 路由表。不匹配的 IS-IS 路由将被阻止进入 IP 路由表，更不会被优选。

配置 IS-IS 路由下发到 IP 路由表过滤的方法是在对应的 IS-IS 进程下通过 **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }**import** 命令进行的，以控制将部分符合条件的 IS-IS 路由下发到 IP 路由表。命令中的参数说明如下。

① *acl-number*：多选一参数，指定用于过滤 IS-IS 路由下发到 IP 路由表的 ACL 列

表号，取值范围为 2 000～2 999 的整数，即仅可以是基本 ACL，用于过滤路由中的目的 IP 地址。

② **acl-name** *acl-name*：多选一参数，指定用于过滤 IS-IS 路由下发到 IP 路由表的 ACL 名称，1～32 的整数，区分大小写，不支持空格。只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对过滤规则有效。

③ **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤 IS-IS 路由下发到 IP 路由表的 IP 地址前缀列表名称，1～169 的整数，区分大小写，不支持空格。

④ **route-policy** *route-policy-name*：多选一参数，指定用于过滤 IS-IS 路由下发到 IP 路由表的路由策略名称，1～40 的整数，区分大小写，不支持空格。

配置该命令后，不会影响本地设备的 LSP 的扩散和 LSDB 的同步，只会影响本地的 IP 路由表，即最终决定有哪些 IS-IS 路由在本地设备上生效。

缺省情况下，没有配置 IS-IS 路由加入 IP 路由表时的过滤策略，可用 **undo filter-policy** [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **import** 命令取消指定的 IS-IS 路由下发到 IP 路由表的过滤配置。

【示例】 使用 ACL 2000 过滤接收的路由，将 1.1.1.0/24 的 IS-IS 路由加入到 IP 路由表中。

```
<Huawei> system-view
[Huawei]acl 2000
[Huawei-acl-basic-2000]rule permit source 1.1.1.0 0.255.255.255
[Huawei] isis
[Huawei-isis-1] filter-policy 2000 import
```

13.7 控制 IS-IS 的路由选路

影响 IS-IS 选路的因素比较多，如 IS-IS 协议的优先级、IS-IS 接口的开销、等价路由的处理方式、IS-IS 路由渗透的配置和 IS-IS 缺省路由的发布，具体可选的配置任务如下。用户可根据具体的应用环境选择其中一项或多项配置任务，通过对这些因素的调整可以实现对路由选择的精确控制。但在配置这些因素之前，也需配置 IS-IS 的基本功能。

① 配置 IS-IS 协议的优先级。

② 配置 IS-IS 接口的开销。

③ 配置 IS-IS 对等价路由的处理方式。

④ 配置 IS-IS 路由渗透。

⑤ 控制 Level-1 设备是否生成缺省路由。

13.7.1 配置 IS-IS 协议的优先级

一台路由器可能会同时运行多个路由协议，这时可能会发现到达同一目的地存在多条不同协议路由，其中协议优先级高的路由将被优选。通过配置 IS-IS 协议的优先级，可以将 IS-IS 路由的优先级提高，使 IS-IS 的路由被优选。如果结合路由策略的使用，还可以灵活地仅将期望的部分 IS-IS 路由的优先级提高，而不影响其他的路由选择。

IS-IS 协议优先级的具体配置方法是在对应的 IS-IS 进程下通过 **preference** { *preference* | **route-policy** *route-policy-name* }* 命令进行的。该命令有三种不同的命令格式和用途。

① **preference** *preference*：为所有 IS-IS 协议的路由设定优先级。

② **preference** *preference* **route-policy** *route-policy-name*：为通过匹配的 IS-IS 路由和没有通过匹配的路由设定不同的优先级。这时通过匹配的路由将采用指定路由策略中 **apply preference** *preference* 子句设定的优先级，而没有通过匹配的 IS-IS 路由将采用 *preference* 参数所设置的优先级。

③ **preference route-policy** *route-policy-name preference*：为通过匹配的路由设定优先级（由 *preference* 参数设置），不影响其他 IS-IS 路由的优先级。

以上三种格式命令中的参数说明如下。

① *preference*：可多选参数，指定 IS-IS 协议的优先级，取值范围为 1～255 的整数，值越小，优先级越高。

② **route-policy** *route-policy-name*：可多选参数，指定用于过滤应用 IS-IS 优先级设置的路由的路由策略名称，1～40 个字符，区分大小写，不支持空格。如果不指定本参数，则本命令的设置将应用于所有 IS-IS 路由。

缺省情况下，IS-IS 协议的优先级为 15，可用 **undo preference** 命令恢复所有 IS-IS 路由为缺省优先级。

【示例 1】设置通过路由策略 abc 的路由优先级被设定为 50，未通过路由策略 abc 的路由优先级被设定为 30。

```
<Huawei> system-view
[Huawei]route-policy abc permit node 1
[Huawei-route-policy]if-match cost 20
[Huawei-route-policy]apply preference 50
[Huawei-route-policy]quit
[Huawei]isis 1
[Huawei-isis-1]preference 30 route-policy abc
```

【示例 2】设置所有 IPv4 IS-IS 路由的优先级均为 25。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] preference 25
```

13.7.2　配置 IS-IS 接口的开销

IS-IS 有三种方式来确定接口的开销，按照优先级由高到低分别如下。

① 接口开销：为单个接口设置开销，优先级最高。

② 全局开销：为所有接口设置开销，优先级中等。

③ 自动计算开销：根据接口带宽自动计算开销，优先级最低。

用户可根据需要选择其中一种或多种接口开销配置方式。在配置接口开销前，可根据实际需要配置 IS-IS 的开销类型，因为不同类型的开销的聚会范围不一样。如果没有为 IS-IS 接口配置任何开销值，IS-IS 接口的默认开销为 10，开销类型是 **narrow**。在实际应用中，为了方便 IS-IS 实现其扩展功能，通常将 IS-IS 的路由开销类型设置为 **wide** 模式。

【经验之谈】**IS-IS 接口开销也即 IS-IS 链路开销，是二层概念，**代表接口所在链路的开销。IS-IS 链路开销（OSPF 中的链路开销也一样）通常是由链路接口的带宽确定的，具体将在下面介绍。**但如果链路两端的接口带宽不一致，则以带宽低的接口来计算整条链路的开销。IS-IS 路由开销是指该路由所经过的链路的链路开销之和，但要注意的是，同一路由器上的不同接口之间的链路开销为 0。**

如果需要修改 IS-IS 的路由开销类型，需在配置 IS-IS 的基本功能时完成 cost-style 的配置，否则在网络运行过程中修改路由开销类型会导致 IS-IS 进程重启，并可能会造成邻居重新建立邻接。

1. 配置 IS-IS 接口开销类型

配置 IS-IS 接口开销类型的方法是在对应的 IS-IS 进程下使用 **cost-style** ｛**narrow** | **wide** | **wide-compatible** | ｛｛**narrow-compatible** | **compatible**｝［**relax-spf-limit**］｝｝命令进行的。命令中的选项说明如下。

① **narrow**：多选一选项，指定 IS-IS 设备所有接口只能接收和发送开销类型为 narrow 的路由。narrow 模式下路由的开销值取值范围为 1～63 的整数。

② **wide**：多选一选项，指定 IS-IS 设备所有接口只能接收和发送开销类型为 wide 的路由。wide 模式下路由的开销值取值范围为 1～16 777 215 的整数。

③ **wide-compatible**：多选一选项，指定 IS-IS 设备所有接口可以接收开销类型为 narrow 和 wide 的路由，但却只发送开销类型为 wide 的路由。

④ **narrow-compatible**：二选一选项，指定 IS-IS 设备所有接口可以接收开销类型为 narrow 和 wide 的路由，但却只发送开销类型为 narrow 的路由。

⑤ **compatible**：二选一选项，指定 IS-IS 设备所有接口可以接收和发送开销类型为 narrow 和 wide 的路由。

⑥ **relax-spf-limit**：可选项，指定 IS-IS 设备所有接口可以接收开销值大于 1 023 的路由，对接口的链路开销值和路由开销值均没有限制，按照实际的路由开销值正常接收该路由。如果不选择此可选项，则会根据具体情况分别进行如下处理。

- 如果路由开销值小于或等于 1 023，且该路由经过的所有接口的链路开销值都小于等于 63，则这条路由的开销值按照实际值接收，即**路由的开销值为该路由所经过的所有接口的链路开销值总和。**
- 如果路由开销值小于或等于 1 023，但该路由经过的所有接口中有的接口链路开销值大于 63，则**设备只能学习到该接口所在设备的其他接口的直连路由和该接口所引入的路由**，路由的开销值按照实际值接收，路由此后要经过的接口将丢弃该路由。此接口之后的路由将被丢弃。
- 如果路由开销值大于 1 023，**设备可以接收链路开销值小于 1 023 的接口所在网段的所有路由**；如果路由开销值大于 1 023，则仅按照 1 023 接收，不能接收链路开销值大于 1 023 的接口所在网段的所有路由。

缺省情况下，IS-IS 设备各接口接收和发送路由的开销类型为 **narrow**，可用 **undo cost-style** 命令恢复 IS-IS 设备各接口接收和发送路由的开销类型为缺省类型。

【**示例**】设置当前 IS-IS 路由器只能发送 narrow 型的报文，但是可以接收 narrow 型和 wide 型的报文。

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] cost-style narrow-compatible
```

2. 配置接口开销

根据前面的介绍，IS-IS 接口的开销可以有三种配置方式，具体配置步骤如表 13-5 所示。一般只需选择一种配置方式，如果同时配置了，则会按照前面介绍的优先级顺序来应用。

表 13-5　IS-IS 接口开销的三种配置方法

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**isis** [*process-id*] 例如：[Huawei] **isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
方式 1：全局开销配置（优先级中等）		
3	**circuit-cost** { *cost* | **maximum** } [**level-1** | **level-2**] 例如：[Huawei-isis-1] **circuit-cost** 30	设置 IS-IS 全局开销。命令中的参数和选项说明如下 ● *cost*：二选一参数，指定接口的链路开销值，当开销类型为 narrow、narrow-compatible 或 compatible 时，取值范围为 1～63 的整数；当开销类型为 wide 或 wide-compatible 时，取值范围为 1～16 777 214 的整数 ● **maximum**：二选一选项，指定接口的链路开销值为最大值——16 777 215，只有当 IS-IS 的开销类型为 wide 或 wide-compatible 模式时才可以选择该选项，此时该接口所在链路上生成的邻居 TLV 不能用于路由计算，仅用于传递 TE 相关信息 ● **level-1**：二选一选项，指定开销值设置仅作用于 L1 链路，如果不指定配置链路开销的链路级别，则开销值设置同时作用于 L1 和 L2 级别的链路，具体要根据对应路由器的类型而定 ● **level-2**：二选一选项，指定开销值设置仅作用于 L2 链路，如果不指定配置链路开销的链路级别，则开销值设置同时作用于 L1 和 L2 级别的链路，具体要根据对应路由器的类型而定 【注意】改变接口的链路开销值，会造成整个网络的路由重新计算，引起流量转发路径变化。 缺省情况下，没有配置所有 IS-IS 接口的链路开销值，可用 **undo circuit-cost** [*cost* | **maximum**] [**level-1** | **level-2**] 命令取消配置的所有 IS-IS 接口的链路开销值
方式 2：自动计算开销配置（优先级最低，**仅适用于 wide 或 wide-compatible 开销类型的接口**）		
3	**bandwidth-reference** *value* 例如：[Huawei-isis-1] **bandwidth-reference** 1000	配置计算带宽的参考值，取值范围为 1～2 147 483 648 的整数，单位是 Mbit/s 【说明】**只有当开销类型为 wide 或 wide-compatible 时**，使用本命令配置的带宽参考值才是有效的，此时各接口的开销值=（bandwidth-reference/接口带宽值）×10；**当开销类型为 narrow、narrow-compatible 或 compatible 时，各个接口的开销值根据表 13-6 来确定** 缺省情况下，带宽参考值为 100 Mbit/s，可用 **undo bandwidth-reference** 命令恢复 IS-IS 接口开销自动计算功能中所使用的带宽参考值为缺省值 100 Mbit/s

（续表）

步骤	命令	说明
4	**auto-cost enable** 例如[Huawei-isis-1] **auto-cost enable**	使能自动计算接口的开销值。当使能此功能后，对于某个IS-IS 接口来说，如果既没有在接口视图下配置其开销值，也没在 IS-IS 视图下配置全局开销值，则此接口的开销由系统自动计算，计算方法见上一步说明 缺省情况下，未使能 IS-IS 根据带宽自动计算接口开销的功能，可用 **undo auto-cost enable** 命令去使能 IS-IS 根据带宽自动计算接口开销的功能
方式 3：接口开销配置（优先级最高）		
3	**quit** 例如：[Huawei-isis-1] **quit**	退出 IS-IS 视图，返回系统视图
4	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入要配置开销的 IS-IS 接口，进入接口视图
5	**isis cost** { *cost* | **maximum** } [**level-1** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis cost 5 level-2**	为 IS-IS 接口设置具体的开销。命令中的参数和选项说明参见本表上面全局开销配置中的 **circuit-cost** 命令中的对应说明，只不过这里的参数和选项仅作用于对应的具体接口，而不是所有 IS-IS 接口 【注意】要改变 Loopback 接口的开销，只能通过本命令进行设置，不能通过上面介绍的全局和自动计算方式配置 缺省情况下，IS-IS 接口的链路开销为 10，可用 **undo isis cost** [*cost* | **maximum**] [**level-1** | **level-2**]命令恢复指定类型链路 IS-IS 接口的开销值为缺省值

IS-IS 接口开销和接口带宽对应关系如表 13-6 所示。

表 13-6　IS-IS 接口开销和接口带宽对应关系

接口开销值	接口带宽范围
60	接口带宽≤10 Mbit/s
50	10 Mbit/s＜接口带宽≤100 Mbit/s
40	100 Mbit/s＜接口带宽≤155 Mbit/s
30	155 Mbit/s＜接口带宽≤622 Mbit/s
20	622 Mbit/s＜接口带宽≤2.5 Gbit/s
10	2.5 Gbit/s＜接口带宽

13.7.3 配置 IS-IS 对等价路由的处理方式

当 IS-IS 网络中有多条冗余链路时，可能会出现多条等价路由，此时有两种配置方式。

① 配置负载分担：流量会被均匀地分配到每条链路上。该方式可以提高网络中链路的利用率，减少某些链路负担过重造成阻塞发生的情况。但是由于对流量转发具有一定的随机性，因此该方式可能不利于对业务流量的管理。

② 配置等价路由优先级：针对等价路由中的每一条路由，明确指定其优先级，优先级高的路由将被优选，优先级低的路由可以作为备用链路。该方式可以在不修改原有配置的基础上，指定某条路由被优选，便于业务的管理，同时可提高网络的可靠性。

以上两种等价路由处理方式的配置步骤如表 13-7 所示。

表 13-7　IS-IS 等价路由处理方式的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**isis** [*process-id*] 例如：[Huawei] **isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
方式 1：配置负载分担方式		
3	**maximum load-balancing** *number* 例如：[Huawei-isis-1] **maximum load-balancing** 2	配置在负载分担方式下的等价路由的最大数量，取值范围会因为不同系列有所不同：AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2201-48FE、AR2202-48FE/2202-48FE-S 和 AR2204/2204-S 的取值范围为 1～4 的整数，AR2220、AR2220L、AR2240/2240-S 和 AR3200 系列的取值范围为 1～8 的整数 【说明】当组网中存在的等价路由数量大于本命令配置的等价路由数量时，将按照下面原则选取有效路由进行负载分担 ● 路由优先级：选取优先级高的等价路由进行负载分担 ● 接口索引：如果路由的优先级相同，则比较接口的编号索引，选取接口索引大的路由进行负载分担 ● 下一跳 IP 地址：如果路由优先级和接口索引都相同，则比较下一跳 IP 地址，选取 IP 地址大的路由进行负载分担 缺省情况下，AR150/150-S/160/200/200-S/1200/1200-S 系列、AR2201-48FE、AR2202-48FE/2202-48FE-S 和 AR2204/2204-S 负载分担方式下的最大等价路由的数量为 4，AR2220、AR2220L、AR2240/2240-S 和 AR3200 系列负载分担方式下的最大等价路由的数量为 8，可用 **undo maximum load-balancing** [*number*]命令删除所有或者指定的负载分担方式下的等价路由数量配置，恢复为缺省配置
方式 2：配置等价路由优先级		
3	**nexthop** *ip-address* **weight** *value* 例如：[Huawei-isis-1]**nexthop** 10.0.0.3 **weight** 1	配置指定等价路由的优先级。命令中的参数说明如下 ● *ip-address*：指定某条等价路由的下一跳 IP 地址，用于确定要配置优先级的等价路由 ● *value*：指定以上指定的等价路由的优先级值，取值范围为 1～254 的整数。值越小，优先级越高 【说明】使用该命令可以配置每条等价路由优先级，在不修改接口开销的情况下，明确指定路由的下一跳，使得该路由被优选。但配置该命令后，IS-IS 设备在转发到达目的网段的流量时，将不采用负载分担方式，而是将所有流量都转发到优先级最高的下一跳 缺省情况下，等价路由的优先级的值为 255，可用 **undo nexthop** *ip-address* 命令取消指定等价路由的优先级设置

13.7.4　配置 IS-IS 路由渗透

如果在一个 L1 区域中有多台 L1/2 设备与 L2 区域相连，每台 L1/2 设备都会在 L1 LSP 中设置 ATT 标志位，则该区域中就有到达 L2 区域和其他 L1 区域的多条出口路由。

说明 ATT 比特标志位是 IS-IS LSP 报文中的一个字段，用来标识 L1 区域是否与其他区域关联。L1/2 设备在其生成的 L1 LSP 中设置该比特位为 1，以通知同一区域中的 L1 设备自己与其他区域相连，也就是说与 L2 骨干区域相连（因为 L1 区域之间不能直接直连）。当 L1 区域中的设备收到 L1/2 设备发送的 ATT 比特位被置位的 L1 LSP 后，它将生成一条指向 L1/2 设备的缺省路由，以便数据可以被路由到其他区域。

缺省情况下，L1 区域的路由会渗透到 L2 区域中，因此 L1/2 设备和 L2 设备了解整个网络的拓扑信息，但 L1 区域的设备只维护本地 L1 区域的 LSDB 数据库，不知道整个网络的拓扑信息。这样一来，L1 路由器只能选择将流量转发到最近（开销最小）的 L1/2 设备，再由 L1/2 设备将流量转发到 L2 区域。然而，该路由可能不是到达目的地的最优路由，因为尽管 L1 路由器到达该 L1/2 的开销是最小的，但该 L1/2 路由器到达目的区域的开销不一定是最小的。

为了帮助 L1 区域内的设备选择到达其他区域的最优路由，可以**在 L1/2 路由器上**配置 IPv4 IS-IS 路由渗透，将 L2 区域的某些路由渗透到本地 L1 区域，这样 L1 区域中的路由器就可以自己根据路由计算选择到达目的区域的最优路由。另外，考虑到网络中部署的某些业务可能只在本地 L1 区域内运行，则无需将这些路由渗透到 L2 区域中，可以**在 L1/2 路由器上**通过配置策略仅将部分 L1 区域的路由渗透到 L2 区域。**在 IS-IS 路由渗透配置方面包括两个方向：一是可以控制由 L2 区域向 L1 区域的路由渗透，同时还可控制 L1 区域向 L2 区域的路由渗透。**

1. 配置 L2 区域的路由渗透到 L1 区域

在 L1/2 路由器上配置 L2 区域的路由渗透到 L1 区域的方法是在对应的 IS-IS 进程下使用 **import-route isis level-2 into level-1** [**tag** *tag* | **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix***ip-prefix-name* | **route-policy** *route-policy-name* }] *命令进行配置。命令中的参数说明如下。

① **tag** *tag*：可多选参数，指定允许渗透的引入的外部路由的标记，取值范围为 1～4 294 967 295 的整数。

② **filter-policy**：可多选选项，指定渗透路由的过滤条件。

③ *acl-number*：多选一参数，指定用来过滤允许渗透的路由的基本 ACL 列表号，取值范围为 2 000～2 999 的整数。

④ **acl-name** *acl-name*：多选一参数，指定用来过滤允许渗透的路由的 ACL 名称，1～32 个字符，区分大小写，不支持空格。只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对过滤规则有效。

⑤ **ip-prefix***ip-prefix-name*：多选一参数，指定用来过滤允许渗透的路由的 IP 地址前缀列表名称，1～19 个字符，区分大小写，不支持空格。

⑥ **route-policy** *route-policy-name*：多选一参数，指定用来过滤允许渗透的路由的路由策略名称，1～40 个字符，区分大小写，不支持空格。

缺省情况下，L2 区域的路由信息不渗透到 L1 区域，可用 **undo import-route isis level-2 into level-1** [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *命令禁止指定的 L2 区域的路由向 L1 区域渗透。

【示例 1】使用名为 2000 的路由策略过滤 IS-IS 从 L2 区域向 L1 区域进行渗透的路由。

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] import-route isis level-2 into level-1 filter-policy 2000
```

2. 配置 L1 区域的路由渗透到 L2 区域

在 L1/2 路由器上配置 L1 区域的路由渗透到 L2 区域的方法是在对应的 IS-IS 进程下使用 **import-route isis level-1 into level-2** [**tag** *tag* | **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix***ip-prefix-name* | **route-policy** *route-policy-name* }] *命令进行配置。命令中的参数说明参见前面的 **import-route isis level-2 into level-1** 命令，只不过此处过滤的是允许向 L1 区域渗透的 L2 区域路由。配置该命令后，只有通过过滤策略的路由才能渗透到 L2 区域中。

缺省情况下，L1 区域的路由信息全部渗透到 L2 区域，可用 **undo import-route isis level-1 into level-2** [**tag** *tag* | **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }] *命令禁止指定的 L1 路由向 L2 区域渗透。

【示例 2】使用名为 2000 的路由策略过滤 IS-IS 从 L1 区域向 L2 区域进行渗透的路由。

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] import-route isis level-1 into level-2 filter-policy 2000
```

13.7.5　控制 Level-1 设备是否生成缺省路由

IS-IS 协议规定，如果 IS-IS L1/2 设备根据其 LSDB 判断到通过 L2 区域比 L1 区域能够到达更多的区域，则该设备会在所发布的 L1 LSP 内将 ATT 比特位置位（即置为 1）。这样，收到这个 ATT 比特位置位的 LSP 报文的 L1 设备会生成一条目的地为发送该 LSP 的 L1/2 设备的缺省路由。

以上是 IS-IS 协议的默认原则，在实际应用中，可以根据需要对 ATT 比特位进行手动配置以更好地为网络服务。这里有两种配置方式：一是在 L1/2 路由器上配置发布的 LSP 报文中 ATT 比特位的置位情况；二是在 L1 路由器上设置在收到 ATT 比特位置位的 L1 LSP 报文后不生成缺省路由。下面具体介绍它们各自的配置方法。

1. 在 L1/2 路由器上配置发布的 LSP 报文中 ATT 比特位的置位情况

在 L1/2 路由器上配置 ATT 比特位的方法是在对应的 IS-IS 进程下通过 **attached-bit advertise** { **always** | **never** }命令进行的。命令中的选项说明如下。

① **always**：二选一选项，设置 ATT 比特位永远置位，缺省情况下收到该 LSP 的 L1 路由器就会生成缺省路由。

② **never**：设置 ATT 比特位永远不置位，避免 L1 路由器生成缺省路由。

说明　虽然 ATT 比特位同时在 L1 LSP 和 L2 LSP 中进行了定义，**但是它只会在 L1 LSP 中被置位，并且只有 L1/2 路由器才会设置这个字段，因此该命令仅对 L1/2 设备生效。**

缺省情况下，L1/2 设备发布的 LSP 的 ATT 比特位根据本节前面介绍的缺省置位规则来决定置位情况，可用 **undo attached-bit advertise** 命令恢复 ATT 比特位缺省置

位规则。

【示例 1】设置 L1/2 设备在 IS-IS 进程 1 中发布的 L1 LSP ATT 比特位永远置位。

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] attached-bit advertise always
```

2. 在 L1 路由器上设置不生成缺省路由

在 L1 路由器上配置在收到 ATT 比特位置位的 L1 LSP 报文后也不生成缺省路由的配置方法是在对应的 IS-IS 进程下通过 **attached-bit avoid-learning** 命令进行配置。通常在配置 L2 区域向 L1 区域进行路由渗透后，要在 L1 路由器上配置不生成缺省路由，以免在与外部区域进行通信时选择了次优路由。

缺省情况下，IS-IS 按 ATT 比特位缺省使用规则生成缺省路由，可用 **undo attached-bit avoid-learning** 命令恢复当 L1 路由器收到 ATT 比特位置位的 LSP 报文时生成缺省路由。

【示例 2】设置 L1 设备不因为收到 ATT 比特位置位的 L1 LSP 报文而生成缺省路由。

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] attached-bit avoid-learning
```

13.8 调整 IS-IS 路由的收敛性能

提高对 IS-IS 网络中故障的响应速度，加快出现网络故障时的路由收敛速度，可以提高 IS-IS 网络的可靠性。通过以下几方面的措施可调整 IS-IS 网络的收敛性能，用户可根据具体的应用环境选择其一项或多项配置任务。但在配置 IS-IS 路由的收敛性能之前，需配置 IS-IS 的基本功能。

① 配置 Hello 报文参数。

② 配置 LSP 报文参数。

③ 配置 CSNP 报文参数。

④ 调整 SPF 的计算时间间隔。

⑤ 配置 IS-IS 路由按优先级收敛。

13.8.1 配置 Hello 报文参数

IS-IS 协议通过 Hello 报文的收发来维护与相邻设备的邻居关系，当本端设备在一段时间（邻居保持时间）内没有收到对端发送的 Hello 报文时，将认为邻居已经失效。所以这里涉及两个时间的配置：一是 Hello 报文的发送时间间隔，二是邻居保持时间。

在 IS-IS 中，本端设备与相邻设备保持邻居关系的时间长短可以通过设置发送 Hello 报文的时间间隔和 IS-IS 的邻居保持时间来控制。

① Hello 报文发送间隔越短，就需要占用越多的系统资源来发送 Hello 报文，造成 CPU 负载过重。

② 如果 IS-IS 的邻居保持时间配置得太大，那么如果对端邻居已经失效，本端设备需要等待过长的时间才能检测到，从而减慢 IS-IS 路由收敛速度。

③ 如果 IS-IS 的邻居保持时间配置得太小，由于网络传输延时和传播差错等原因可能会造成个别 Hello 报文的丢失或出错，那么邻居关系会频繁地在 Up 和 Down 之间变化，造成 IS-IS 网络的路由振荡。

通常是建议 IS-IS 网络中的所有设备配置相同的 Hello 报文发送间隔和邻居保持时间，以免造成某些设备对链路故障的检测速度低于其他设备而减慢全网 IS-IS 路由的收敛速度。

Hello 报文发送时间间隔和邻居保持时间的配置步骤如表 13-8 所示（**各配置任务之间没有严格的先后配置次序**）。

表 13-8　　Hello 报文参数的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**interface** *interface-type interface-number* 例如: [Huawei] **interface** gigabitethernet 1/0/0	键入要配置 Hello 报文发送时间间隔的 IS-IS 接口，进入接口视图。需要先通过 **isis enable** 命令在该接口上使能 IS-IS 功能，具体参见 13.3.1 小节
设置 Hello 报文发送时间间隔	3	**isis timer hello** *hello-interval* [**level-1** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis timer hello** 20 **level-2**	（可选）配置接口上 Hello 报文的发送间隔。命令中的参数和选项说明如下 ● *hello-interval*：设置接口发送 Hello 报文的时间间隔，取值范围为（3～255）整数秒 ● **level-1**：二选一选项，设置以上 Hello 报文发送时间间隔的设置仅适用于 L1 级别 Hello 报文，如果没有指定级别，则将同时作用于 L1 和 L2 级别 Hello 报文。**仅可在广播接口上配置，在点到点链路上，只有一种 Hello 报文，不需要指定 L1 和 L2 级别** ● **level-2**：二选一选项，设置以上 Hello 报文发送时间间隔的设置仅适用于 L2 级别 Hello 报文，如果没有指定级别，则将同时作用于 L1 和 L2 级别 Hello 报文。**也仅可在广播接口上配置，在点到点链路上，只有一种 Hello 报文，不需要指定 L1 和 L2 级别** 缺省情况下，IS-IS 接口发送 Hello 报文的间隔时间是 10 s，可用 **undo isis timer hello** [*hello-interval*] [**level-1** | **level-2**]命令恢复 IS-IS 接口指定级别的 Hello 报文发送间隔时间为缺省值
设置邻居保持时间	4	**isis timer holding-multiplier** *number* [**level-1** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis timer holding-multiplier** 6 **level-2**	（可选）配置 Hello 报文的发送间隔时间的倍数，以达到修改 IS-IS 的邻居保持时间的目的。命令中的参数和选项说明如下 ● *number*：指定邻居保持时间为 Hello 报文的发送间隔时间的倍数，取值范围为 3～1 000 的整数 ● **level-1**：二选一选项，以上 Hello 报文发送时间间隔的倍数设置仅适用于 L1 级别 Hello 报文，如果没有指定级别，则将同时作用于 L1 和 L2 级别 Hello 报文。**仅可在广播接口上配置，在点到点链路上，只有一种 Hello 报文，不需要指定 L1 和 L2 级别**

（续表）

配置任务	步骤	命令	说明
设置邻居保持时间	4	**isis timer holding-multiplier** *number* [**level-1** | **level-2**] 例如：[Huawei-GigabitEthernet1/0/0] **isis timer holding-multiplier** 6 **level-2**	• **level-2**：二选一选项，以上 Hello 报文发送时间间隔的倍数设置仅适用于 L2 级别 Hello 报文，如果没有指定级别，则将同时作用于 L1 和 L2 级别 Hello 报文。**也仅可在广播接口上配置，在点到点链路上，只有一种 Hello 报文，不需要指定 L1 和 L2 级别** 缺省情况下，Hello 报文的发送间隔时间的倍数值为 3，即邻居保持时间为 Hello 报文的发送间隔时间的 3 倍，可用 **undo isis timer holding-multiplier** [*number*] [**level-1** | **level-2**] 命令恢复指定级别的 Hello 报文的发送间隔时间的倍数为缺省值 【说明】如果通过 **isis circuit-type** 命令将广播接口模拟为 P2P 接口或者通过 **undo isis circuit-type** 命令将该接口恢复为广播接口，则邻居保持时间相对于 Hello 报文的发送间隔时间的倍数恢复为缺省值

13.8.2 配置 LSP 报文参数

LSP 报文用于交换链路状态信息，可以配置 LSP 报文的大小及最大有效时间，还可以通过使能 LSP 加速扩散，以及减小接口发送 LSP 报文的最小时间间隔和 LSP 报文的刷新周期加快 LSP 报文的扩散速度，使得网络快速收敛。还可以通过配置 LSP 生成的智能定时器，自动根据网络环境计算出生成 LSP 报文的时间间隔，这样既可以快速响应突发事件，加快网络的收敛速度，又可以在网络变化频繁时自动延长智能定时器的间隔时间，避免过度占用 CPU 资源。这些参数的具体说明如表 13-9 所示。

表 13-9　　LSP 报文参数说明

配置的参数	作用	说明
LSP 报文的大小	控制生成和接受 LSP 报文的大小	当链路状态信息变大时，可以增大生成 LSP 报文的长度，使得每个 LSP 报文可以携带更多的信息
LSP 报文的最大有效时间	控制 LSP 报文的最大有效时间，保证在未收到更新的 LSP 之前旧 LSP 报文的有效性	在路由器向邻居发送自己生成的 LSP 报文时，会在其中填写此 LSP 报文的最大有效时间，接收路由器可根据此时间来计算出认为该 LSP 无效的时间。当此 LSP 被邻居路由器接收后，它的有效时间会随着时间的变化不断减小。如果邻居路由器一直没有收到源路由器的 LSP 报文更新，而原来的 LSP 报文的有效时间已减少到 0，则该 LSP 再继续保持 60 s，如果还没收到新的 LSP，那么此 LSP 将被从邻居路由器的 LSDB 中删除
LSP 报文的刷新周期	控制 LSP 报文的泛洪定时刷新，保持 LSBD 的同步	IS-IS 网络主要通过 LSP 报文的泛洪实现链路状态的同步。泛洪是指一个路由器向相邻路由器发送自己的 LSP 报文后，相邻路由器再将同样的 LSP 报文传送到除发送该 LSP 报文的路由器外的其他邻居的逐级扩展方式。这样就可以一级一级地将 LSP 报文传送到整个层次（L1 路由或者 L2 路由），使整个层次内的每一个路由器就都可以拥有相同的 LSP 信息，并保持 LSDB 的同步
接口发送 LSP 报文的最小时间间隔	控制在 LSP 报文刷新时单个 LSP 报文之间的发送间隔	减小发送 LSP 报文的最小时间间隔可以加快 LSP 报文的扩散速度，但这样会加重设备的 CPU 负担，也可能频繁引起网络振荡

（续表）

配置的参数	作用	说明
LSP 报文生成的智能定时器	智能控制 LSP 报文生成的频率，平衡提高收敛速度与减轻系统负荷之间的关系	在运行 IS-IS 的网络中，当本地路由信息发生变化时，路由器需要产生新的 LSP 报文来通告这些变化。但当本地路由信息变化比较频繁时，这样做会占用大量的系统资源。为了加快网络的收敛速度，同时又不影响系统性能，可通过配置 LSP 报文生成的智能定时器，使路由器可根据路由信息的变化频率自动调整生成 LSP 报文的延迟时间（不是固定的）
LSP 报文快速扩散	控制接口每次扩散 LSP 报文的数量，以便加快 IS-IS 网络的收敛速度	缺省情况下，当 IS-IS 收到其他路由器发来的 LSP 报文时，如果此 LSP 报文比本地 LSDB 中相应的 LSP 报文版本要新，则更新 LSDB 中的 LSP 报文，并用一个定时器定期将 LSDB 内已更新的 LSP 报文扩散出去。LSP 快速扩散特性改进了这种方式，可使设备在收到一个或多个比较新的 LSP 报文时，在路由计算之前，先将小于指定数目的 LSP 报文扩散出去，加快 LSDB 的同步过程
点到点链路上的 LSP 报文重传时间间隔	控制 LSP 报文的重传间隔，保证点到点网络中 LSDB 的同步	在 P2P 网络中，链路两端的设备通过 LSP 报文扩散达到 LSDB 的同步。链路其中一端的设备发送 LSP 报文，如果另一端的设备收到该 LSP 报文，则回复 PSNP 报文进行确认。如果在一定时间内，发送报文的设备未收到对端的 PSNP 确认报文，则会重新发送该 LSP 报文

以上 LSP 报文参数的具体配置步骤如表 13-10 所示（**各配置任务之间没有严格的先后配置次序，且均为可选配置**）。

表 13-10　　LSP 报文参数的配置步骤

配置任务	步骤	命令	说明
公共配置步骤	1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
	2	**isis** [*process-id*] 例如：[Huawei] **isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
配置 LSP 的大小	3	**lsp-length** { **originate** | **receive** } *max-size* 例如：[Huawei-isis-1] **lsp-length originate** 1024	配置当前 IS-IS 路由器生成的 LSP 报文的最大长度和接收 LSP 报文的最大长度。命令中的参数和选项说明如下 • **originate**：二选一选项，指定配置生成的 LSP 报文的最大长度 • **receive**：二选一选项，指定配置接收的 LSP 报文的最大长度 • *max-size*：指定 LSP 报文的最大长度，取值范围为 512～16 384 整数个字节 【注意】所配置的生成的 LSP 报文的最大长度必须小于或等于所配置的接收的 LSP 报文的最大长度。并且要注意：以太网接口的 MTU 值要大于或等于最大长度值加 3；P2P 接口的 MTU 值要大于或等于最大长度值。由于目前接口支持的 MTU 最大值是 9 600 字节，因此，为了实现两端的正常通信，LSP 的报文最大长度（包括生成和接收）允许的最大取值为 9 600–3=9 597 字节

（续表）

配置任务	步骤	命令	说明
配置 LSP 的大小	3	**lsp-length** { **originate** | **receive** } *max-size* 例如：[Huawei-isis-1] **lsp-length originate** 1024	缺省情况下，IS-IS 路由器生成的 LSP 报文和接收的 LSP 报文长度均为 1 497 字节，可用 **undo lsp-length** { **originate** | **receive** }命令恢复当前 IS-IS 路由器生成 LSP 报文的长度或者接收 LSP 报文的长度为缺省值
配置 LSP 的最大有效时间	4	**timer lsp-max-age** *age-time* 例如：[Huawei-isis-1] **timer lsp-max-age** 1500	配置当前 IS-IS 进程生成的 LSP 的最大有效时间，取值范围为 2～65 535 的整数秒 缺省情况下，LSP 的最大有效时间为 1 200 s，可用 **undo timer lsp-max-age** 命令恢复当前 IS-IS 进程生成的 LSP 的最大有效时间为缺省值
配置 LSP 的刷新周期	5	**timer lsp-refresh** *refresh-time* 例如：[Huawei-isis-1] **timer lsp-refresh** 1200	配置 LSP 的刷新周期，取值范围为 1～65 534 的整数秒 缺省情况下，LSP 的刷新周期是 900 s，可用 **undo timer lsp-refresh** 命令恢复 LSP 的刷新周期为缺省值
配置 LSP 快速扩散	6	**flash-flood** [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]] 例如：[Huawei-isis-1] **flash-flood** 6 **max-timer-interval** 100	使能 LSP 报文的快速扩散特性，以便加快 IS-IS 网络的收敛速度。命令中的参数和选项说明如下 ● *lsp-count*：可多选参数，指定每个接口一次扩散 LSP 的最大数量，取值范围为 1～15 的整数，缺省值是 5 ● **max-timer-interval** *interval*：可多选参数，指定 LSP 扩散的最大间隔时间，取值范围为 10～50 000 的整数毫秒，缺省值是 10 ms。配置此定时器后，在路由计算之前如果这个定时器未超时，则立即扩散；否则在该定时器超时后发送 ● **level-1**：二选一选项，指定以上设置仅作用于 L1 LSP 报文，如果没有指定级别，则缺省以上设置同时作用于 L1 和 L2 LSP 报文 ● **level-2**：二选一选项，指定以上设置仅作用于 L2 LSP 报文，如果没有指定级别，则缺省以上设置同时作用于 L1 和 L2 LSP 报文 缺省情况下，未使能 LSP 快速扩散特性，可用 **undo flash-flood** [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]]*命令去使能指定级别 LSP 报文的快速扩散特性
配置 LSP 生成的智能定时器	7	**timer lsp-generation** *max-interval* [*init-interval* [*incr-interval*]] [**level-1** | **level-2**] 例如：[Huawei-isis-1] **timer lsp-generation** 20 50 2000	配置 LSP 生成智能定时器。命令中的参数和选项说明如下 ● *max-interval*：指定产生具有相同的 LSP ID 的 LSP 报文的最大延迟时间，取值范围为 1～120 的整数秒，缺省值为 2 ● *init-interval*：可选参数，指定初次触发产生 LSP 报文的延迟时间，取值范围为 1～60 000 的整数毫秒，缺省情况下不使用这个延迟时间。如果只选择此参数，则智能定时器退化为一般的一次性触发定时器 ● *incr-interval*：可选参数，指定两次产生具有相同的 LSP ID 的 LSP 报文之间的递增延迟时间，取值范围为 1～60 000 的整数毫秒，缺省情况下不使用这个延迟时间

（续表）

配置任务	步骤	命令	说明
配置 LSP 生成的智能定时器	7	**timer lsp-generation** *max-interval* [*init-interval* [*incr-interval*]] [**level-1** | **level-2**] 例如：[Huawei-isis-1] **timer lsp-generation** 20 50 2000	• **level-1**：二选一选项，指定以上设置仅作用于 L1 LSP 报文，如果没有指定级别，则缺省以上设置同时作用于 L1 和 L2 LSP 报文 • **level-2**：二选一选项，指定以上设置仅作用于 L2 LSP 报文，如果没有指定级别，则缺省以上设置同时作用于 L1 和 L2 LSP 报文 【说明】在配置以上参数时要注意以下几个注意事项 • 如果同时配置了 *init-interval* 及 *incr-interval* 参数时，初次产生 LSP 报文的延迟时间为 *init-interval*；第二次产生具有相同 LSP ID 的 LSP 报文的延迟时间为 *incr-interval*。随后，路由每变化一次，产生 LSP 报文的延迟时间都增大为前一次的两倍，直到 *max-interval*。稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval* • 如果配置了 *init-interval* 参数，但没有配置 *incr-interval* 参数，则初次产生 LSP 报文时使用 *init-interval* 作为延迟时间，随后都是使用 *max-interval* 作为延迟时间。同样，稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval* • 如果所配置的产生 LSP 的延迟时间过长，则本地路由信息的变化无法及时通告给邻居，导致网络的收敛速度变慢 缺省情况下，没有配置 LSP 生成智能定时器，可用 **undo timer lsp-generation** [*max-interval* [*init-interval* [*incr-interval*]]] [**level-1** | **level-2**]命令取消配置指定的 LSP 生成的智能定时器
	8	**quit** 例如：[Huawei-isis-1] **quit**	退出 IS-IS 视图，进入接口视图
配置接口发送 LSP 的最小时间间隔	9	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入要配置 LSP 报文参数的 IS-IS 接口，进入接口视图。需要先通过 **isis enable** 命令在该接口上使能 IS-IS 功能，具体参见 13.3.1 小节
	10	**isis timer lsp-throttle** *throttle-interval* [**count** *count*] 例如：[Huawei-GigabitEthernet1/0/0] **isis timer lsp-throttle** 500	配置 IS-IS 接口发送 LSP 报文的最小间隔时间和此时间内发送的最大的报文数。命令中的参数说明如下 • *throttle-interval*：指定接口发送 LSP 报文的最小间隔时间，取值范围为 1～10 000 的整数毫秒 • **count** *count*：可选参数，指定在 *throttle-interval* 时间间隔内发送 LSP 报文的最大数目，取值范围为 1～1 000 的整数 缺省情况下，接口上发送 LSP 报文的最小间隔时间是 50 ms，每次发送 LSP 报文的最大数目是 10，可用 **undo isis timer lsp-throttle** 命令恢复 IS-IS 接口发送 LSP 报文的最小间隔时间和此时间内发送的最大的报文数为缺省值

（续表）

配置任务	步骤	命令	说明
配置点到点链路上的LSP重传时间间隔	11	**isis circuit-type p2p** 例如：[Huawei-GigabitEthernet1/0/0] **isis circuit-type p2p**	（可选）将IS-IS广播网接口的网络类型模拟为P2P类型。如果接口已是P2P类型，则不需要执行本步 缺省情况下，接口网络类型根据物理接口决定，可用 **undo isis circuit-type** 命令恢复IS-IS接口的缺省网络类型
	12	**isis timer lsp-retransmit** *retransmit-interval* 例如：[Huawei-GigabitEthernet 1/0/0] **isis timer lsp-retransmit** 10	配置点到点链路上LSP报文的重传间隔时间，取值范围为1～300的整数秒 【说明】**由于只有点到点网络中设备才会发送PSNP报文进行确认，因此本命令只能配置设备在点到点接口上才有效** 在点到点网络中，链路两端的设备通过LSP扩散达到LSDB的同步。链路其中一端的设备发送LSP报文，如果另一端的设备收到该LSP报文，则回复PSNP报文进行确认。如果在一定时间内，发送报文的设备未收到对端的PSNP确认报文，则会重新发送该LSP报文 本命令可以用来配置设备重新发送LSP报文的间隔时间。配置该命令后，设备发送LSP报文后，会等待时间间隔 *retransmit-interval*。在这段时间内，如果收到对端的PSNP确认报文，则不会重传该LSP报文，否则重传该LSP报文 缺省情况下，点到点链路上LSP报文的重传间隔时间为5 s，可用 **undo isis timer lsp-retransmit** 命令恢复点到点链路上LSP报文的重传间隔时间为缺省值

13.8.3 配置CSNP报文参数

CSNP（全序列号报文）包括本地设备上某个LSDB中所有的LSP摘要信息，用来保证相邻设备间LSDB的同步。在广播网链路和点到点链路中，CSNP的运行机制略有不同。

① 在广播网络中，CSNP是由DIS设备周期性发送的。当邻居发现LSDB不同步时，向DIS发送PSNP报文来请求缺失的LSP报文。

② 在P2P网络中，CSNP只在第一次建立邻接关系时发送。

正因为在P2P网络中CSNP报文仅发送一次，所以CSNP报文参数仅可在广播网络中配置，而且仅可配置CSNP报文的发送时间间隔。由于IS-IS路由的收敛速度依赖于LSDB的同步速度，因此减小CSNP报文的发送间隔时间可以加快LSDB的同步以及IS-IS路由的收敛。但是如果该值设置过小，则DIS会频繁发送CSNP报文，从而造成设备的CPU、内存及网络带宽占用过高，影响正常业务的运行。

在广播网络中，CSNP报文参数的具体配置方法是在对应的接口（当然该接口必须是已使能了IS-IS功能的接口）视图下使用 **isis timer csnp** *csnp-interval* [**level-1** | **level-2**] 命令进行的。命令中的参数和选项说明如下。

① *csnp-interval*：指定 CSNP 报文在广播网络中发送的间隔时间，取值范围为 1～65 535 的整数秒。

② **level-1**：二选一选项，指定以上 CSNP 报文发送时间间隔配置仅作用于 L1 CSNP，如果不指定则将同时作用于 L1 CSNP 和 L2 CSNP。

③ **level-2**：二选一选项，指定以上 CSNP 报文发送时间间隔配置仅作用于 L2 CSNP，如果不指定则将同时作用于 L1 CSNP 和 L2 CSNP。

缺省情况下，在广播网络上发送 CSNP 报文的间隔时间是 10 s，可用 **undo isis timer csnp** [*csnp-interval*] [**level-1** | **level-2**] 命令恢复指定级别 CSNP 报文发送时间间隔为缺省值。如果通过 **undo isis circuit-type** 命令将某 IS-IS 接口恢复为广播接口，则该接口的 IS-IS 发送 CSNP 报文的间隔时间也将恢复为缺省值。

【示例】设置 L2 的 CSNP 报文在接口 GE1/0/0 上每 15 s 发送一次。

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer csnp 15 level-2
```

13.8.4 调整 SPF 的计算时间间隔

当网络变化比较频繁时，IS-IS 会频繁地进行 SPF 计算，而这样会消耗系统大量的 CPU 资源，影响其他业务的运行。这时可通过配置智能定时器灵活调整不同时期 SPF 路由计算的时间间隔，这样可使路由器在刚开始进行 SPF 计算时，两次计算的间隔时间较小，保证 IS-IS 路由的收敛速度，而这之后随着整个 IS-IS 网络的拓扑趋于稳定时，就可以适当地延长两次 SPF 计算的间隔时间，从而减少不必要的资源消耗。具体的配置步骤如表 13-11 所示。

表 13-11　　SPF 计算智能定时器的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**isis** [*process-id*] 例如：[Huawei] **isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
3	**timer spf** *max-interval* [*init-interval* [*incr-interval*]] 例如：[Huawei-isis-1] **timer spf** 15 10 5000	设置 SPF 计算智能定时器。命令中的参数说明如下 • *max-interval*：指定路由计算最大延迟时间，取值范围为 1～120 的整数秒，缺省值是 5 s • *init-interval*：可选参数，指定初次路由计算的延迟时间，取值范围为 1～60 000 的整数毫秒，缺省值是 50 ms。缺省情况下不使用这个延迟时间。如果不指定 *init-interval*，智能定时器就退化为一般的一次性触发定时器 • *incr-interval*：可选参数，指定两次路由计算之间的递增延迟时间。如果不指定 *incr-interval*，初次进行 SPF 计算用 *init-interval* 作为延迟时间，随后都是使用 *max-interval* 作为延迟时间，取值范围为 1～60 000 的整数毫秒，缺省值是 200 ms。如果不指定本参数，初次进行 SPF 计算用

（续表）

步骤	命令	说明
3	**timer spf** *max-interval* [*init-interval* [*incr-interval*]] 例如：[Huawei-isis-1] **timer spf** 15 10 5000	*init-interval* 作为延迟时间，随后都是使用 *max-interval* 作为延迟时间 【说明】如果同时配置 *init-interval* 和 *incr-interval* 参数，则初次进行 SPF 计算的延迟时间为 *init-interval*；第二次进行 SPF 计算的延迟时间为 *incr-interval*。随后，每变化一次，SPF 计算的延迟时间增大为前一次的两倍，直到 *max-interval* 稳定在 *max-interval* 三次或者 IS-IS 进程被重启，延迟时间又降回到 *init-interval* 缺省情况下，SPF 路由计算的最大延迟时间为 5 s，可用 **undo timer spf** 命令恢复 SPF 计算的最大延迟时间为缺省值
4	**spf-slice-size** *duration-time* 例如：[Huawei-isis-1] **spf-slice-size** 50	（可选）配置 IS-IS 每次路由计算的最大持续时间，取值范围为 1～5 000 的整数毫秒 当路由表中的路由数目非常多时，为防止路由计算占用系统资源的时间过长，可以通过本命令来缩短每次路由计算的最大持续时间 缺省情况下，每次路由计算的最大持续时间为 2 ms，可用 **undo spf-slice-size** 命令恢复每次路由计算的最大持续时间为缺省配置

13.8.5 配置 IS-IS 路由按优先级收敛

随着网络的融合，区分服务的需求越来越强烈。某些路由可以指导关键业务的转发，如 VoIP、视频会议、组播等，这些关键的业务路由需要尽快收敛，而非关键路由可以相对慢一点收敛。因此，系统需要对不同路由按不同的收敛优先级处理，来提高网络可靠性。

系统为路由设置了不同的收敛优先级，分为 critical、high、medium、low 4 种，其中 critical 路由的收敛优先级最高，low 路由的收敛优先级最低，系统根据这些路由的收敛优先级采用相对的优先收敛原则，即按照一定的调度比例进行路由收敛安装，指导业务的转发。

AR G3 系列路由器支持通过配置 IS-IS 路由的收敛优先级，使某些重要路由在网络拓扑发生变化时优先收敛。IS-IS 路由收敛优先级的应用规则如下。

① 对于已存在的 IS-IS 路由，收敛优先级将依据以下将要介绍的 **prefix-priority** 命令重新进行设置。

② 对新增加的 IS-IS 路由，收敛优先级将依据以下将要介绍的 **prefix-priority** 命令的过滤结果进行设置。

③ 如果一条路由符合多个收敛优先级的匹配规则，则这些收敛优先级中最高者当选为路由的收敛优先级。

④ L1 IS-IS 路由的收敛优先级高于 L2 IS-IS 路由的收敛优先级。

配置 IS-IS 路由按优先级收敛的步骤如表 13-12 所示。

表 13-12　**IS-IS 路由按优先级收敛的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**isis** [*process-id*] 例如：[Huawei] **isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
3	**prefix-priority** [**level-1** | **level-2**] { **critical** | **high** | **medium** } { **ip-prefix** *prefix-name* | **tag** *tag-value* } 例如：[Huawei-isis-1] **prefix-priority level-1 critical tag** 3	配置 IS-IS 路由（包括 IS-IS 主机路由和缺省路由）的收敛优先级。命令中参数和选项说明如下 ● **level-1**：二选一可选项，指定设置 L1 级别的 IS-IS 路由的收敛优先级，如果没有指定路由级别，则同时为 L1 和 L2 级别的 IS-IS 路由设置收敛优先级 ● **level-2**：二选一可选项，指定设置 L2 级别的 IS-IS 路由的收敛优先级，如果没有指定路由级别，则同时为 L1 和 L2 级别的 IS-IS 路由设置收敛优先级 ● **critical**：多选一选项，指定 IS-IS 路由的收敛优先级为 critical（最高级别） ● **high**：多选一选项，指定 IS-IS 路由的收敛优先级为 high（高级别） ● **medium**：多选一选项，指定 IS-IS 路由的收敛优先级为 medium（中级别） ● **ip-prefix***prefix-name*：二选一参数，指定用于过滤要设置收敛性能的 IS-IS 路由的 IP 地址前缀列表名称，1～169 个字符，区分大小写，不支持空格 ● **tag** *tag-value*：二选一参数，指定用于过滤要设置收敛性能的 IS-IS 路由的标记，取值范围为 1～4 294 967 295 的整数 缺省情况下，IS-IS 主机路由和缺省路由的收敛优先级为 medium，其他 IS-IS 路由的收敛优先级为 low，可用 **undo prefix-priority** [**level-1** | **level-2**] { **critical** | **high** | **medium** } 命令恢复指定级别的 IS-IS 路由为缺省收敛优先级
4	**quit** 例如：[Huawei-isis-1] **quit**	退出 IS-IS 视图，返回系统视图
5	**ip route prefix-priority-scheduler** *critical-weight high-weight medium-weight low-weight* 例如：[Huawei] **ip route prefix-priority-scheduler** 10 2 1 1	（可选）配置 IPv4 路由按优先级调度的比例。为了防止高优先级路由过多而导致低优先级路由迟迟得不到处理进而影响网络的性能，可运行本命令来调整 IPv4 路由按优先级调度的比例。命令中的参数说明如下 ● *critical-weight*：指定 Critical 队列的调度加权值（也就是比重），取值范围为 1～10 的整数 ● *high-weight*：指定 High 队列的调度加权值，取值范围为 1～10 的整数 ● *medium-weight*：指定 Medium 队列的调度加权值，取值范围为 1～10 的整数 ● *low-weight*：指定 Low 队列的调度加权值，取值范围为 1～10 的整数 缺省情况下，IPv4 路由按优先级调度的比例为 8:4:2:1，可用 **undo ip route prefix-priority-scheduler** 命令恢复 IPv4 路由按优先级调度为缺省比例

13.9 提高 IS-IS 网络的安全性

在对安全性要求较高的网络中，可以通过配置 IS-IS 认证来提高 IS-IS 网络的安全性。IS-IS 认证包括接口认证、区域认证、路由域认证三种，还可配置 optional checksum TLV 校验和认证（用得比较少，在此不作介绍）。但在配置 IS-IS 网络安全性之前，需配置 IS-IS 的基本功能。

13.9.1 配置 IS-IS 接口认证

通常情况下，IS-IS 不对发送的 IS-IS 报文封装认证信息，也不对收到的报文做认证检查。这样，当有恶意报文对网络进行攻击时可能会导致整个网络的信息被窃取，因此，需要配置 IS-IS 认证提高网络的安全性。

通过配置 IS-IS 接口认证，可以封装认证信息到 Hello 报文中，以确认邻居的有效性和正确性。IS-IS 接口认证包括简单认证、MD5 认证、HMAC-SHA256 认证和 Keychain（密钥链）认证几种模式，具体的配置步骤如表 13-13 所示（**需要在邻居设备同一链路上的 IS-IS 接口上配置相同的认证模式和密码**）。

表 13-13 IS-IS 接口认证的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**interface** *interface-type interface-number* 例如：[Huawei]**interface** gigabitethernet 1/0/0	键入要配置接口认证的 IS-IS 接口，进入接口视图。需要先通过 **isis enable** 命令在该接口上使能 IS-IS 功能，具体参见 13.3.1 小节
3	**isis authentication-mode simple** { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**ip**| **osi**] [**send-only**] 例如：[Huawei-GigabitEthernet1/0/0] **isis authentication-mode simple** huawei	（四选一）配置 IS-IS 接口的简单认证模式。命令中的参数和选项说明如下 ● **plain** *plain-text*：二选一参数，指定简单认证的明文密码，1～16 个字符，可以为字母或数字，区分大小写，不支持空格。**此模式下只能键入明文密码，密码将以明文形式保存在配置文件中** ● **cipher**：可选项，指定为密文密码，此时可以键入明文或密文密码，但在查看配置文件时以密文方式显示 ● *cipher-text*：二选一参数，指定简单认证的密文密码，可以为字母或数字，区分大小写，不支持空格，长度为 1～16 位明文密码或 32 位密文密码 ● **level-1**：二选一可选项，指定所设置的认证密码仅作用于 L1 级 IS-IS Hello 报文交互认证，如果不指定报文级别，则同时作用于 L1 和 L2 级 IS-IS Hello 报文交互认证。**仅在 WAN 侧以太网接口和 LAN 侧 VLANIF 接口上是可见的** ● **level-2**：二选一可选项，指定所设置的认证密码仅作用于 L2 级 IS-IS Hello 报文交互认证，如果不指定报文级别，则同时作用于 L1 和 L2 级 IS-IS Hello 报文交互认证。**仅在 WAN 侧以太网接口和 LAN 侧 VLANIF 接口上是可见的**

（续表）

步骤	命令	说明
3	**isis authentication-mode simple** { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**ip**| **osi**] [**send-only**] 例如：[Huawei-GigabitEthernet1/0/0] **isis authentication-mode simple** huawei	• **ip**：二选一可选项，指定所设置的认证密码仅作用于 IP 网络，如果不指定网络类型，则缺省仅作用于 OSI 网络 • **osi**：二选一可选项，指定所设置的认证密码仅作用于 OSI 网络，如果不指定网络类型，则缺省仅作用于 OSI 网络 • **send-only**：可选项，指定仅对发送的 Hello 报文加载认证信息，不对接收的 Hello 报文进行认证。此时，仅当在本端不需要进行认证检查且对端认证通过时才可以建立起邻居关系。如果不指定此参数，则缺省为对发送的 Hello 报文加载认证信息且对接收的 Hello 报文进行认证。**此时应保证同一网络所有接口的相同级别的认证密码一致** 缺省情况下，IS-IS 的 Hello 报文中不添加认证信息，对接收到的 Hello 报文也不做认证，可用 **undo isis authentication-mode simple** { **plain** *plain-text* | **cipher** *plain-cipher-text* } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]命令取消简单认证，同时删除 Hello 报文中的简单认证信息
	isis authentication-mode md5 { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**ip** |**osi**] [**send-only**] 例如：[Huawei-GigabitEthernet1/0/0] **isis authentication-mode md5** huawei	（四选一）配置 IS-IS 接口的 MD5 认证模式。命令中的参数和选项说明如下 • **plain** *plain-text*：二选一可选参数，指定认证的明文密码，1～255 个字符，可以为字母或数字，区分大小写，不支持空格。此模式下只能键入明文密码，密码将以明文形式保存在配置文件中 • **cipher**：可选项，指定为密文密码，此时可以键入明文或密文密码，但在查看配置文件时以密文方式显示 • *cipher-text*：二选一可选参数，指定简单认证的密文密码，可以为字母或数字，区分大小写，不支持空格，长度为 1～255 位明文密码或 20～392 位密文密码 **其他参数和选项说明参见上面介绍的简单认证模式配置命令** 缺省情况下，IS-IS 的 Hello 报文中不添加认证信息，对接收到的 Hello 报文也不做认证，可用 **undo isis authentication-mode md5** { **cipher** *plain-cipher-text* | **plain** *plain-text* } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]命令取消 MD5 认证，同时删除 Hello 报文中的 MD5 认证信息
	isis authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**send-only**] 例如：[Huawei-GigabitEthernet1/0/0] **isis authentication-mode hmac-sha256** 1 huawei	（四选一）配置 IS-IS 接口的 HMAC-SHA256 认证模式。命令中的 *key-id* 参数用来指定 HMAC-SHA256 算法的密钥 ID，取值范围为 0～65 535 的整数。**其他参数和选项说明参见上面介绍的 MD5 认证模式配置命令** 缺省情况下，IS-IS 的 Hello 报文中不添加认证信息，对接收到的 Hello 报文也不做认证，可用 **undo isis authentication-mode hmac-sha256 key-id** *key-id* { **plain** *plain-text* | **cipher** *plain-cipher-text* } [**level-1** | **level-2**] [**send-only**]命令取消 HMAC-SHA256 认证，同时删除 Hello 报文中的 HMAC-SHA256 认证信息

（续表）

步骤	命令	说明
3	**isis authentication-mode keychain** *keychain-name* [**level-1** | **level-2**] [**send-only**] 例如：[Huawei-GigabitEthernet1/0/0] **isis authentication-mode keychain** isiskey	（四选一）配置 IS-IS 接口的 Keychain 认证模式。命令中的参数 *keychain-name* 用来指定 Keychain 名称，1～47 个字符，不区分大小写，不支持空格。**其他选项说明参见前面介绍的简单认证模式配置命令** 【说明】所使用的 Keychain（密钥链）需已使用 **keychain** *keychain-name* 命令创建，然后分别通过 **key-id** *key-id*、**key-string** { [**plain**] *plain-text* | [**cipher**] *cipher-text* }和 **algorithm** { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }命令配置该 keychain 采用的 key-id、密码及其认证算法，必须保证本端和对端的 key-id、algorithm、key-string 相同，才能建立 IS-IS 邻居 缺省情况下，IS-IS 的 Hello 报文中不添加认证信息，对接收到的 Hello 报文也不做认证，可用 **undo isis authentication-mode keychain** *keychain-name* [**level-1** | **level-2**] [**send-only**] 命令取消 Keychain 认证，同时删除 Hello 报文中的 Keychain 认证信息

13.9.2 配置区域或路由域的认证

区域认证会将认证密码封装在 L1 区域的 IS-IS 报文（**非 Hello 报文**）中，只有通过认证的报文才会被接收。因此，**当需要对 L1 区域进行认证时，需要对该 L1 区域所有 IS-IS 设备（包括 L1 设备和 L1/2 设备）配置 IS-IS 区域认证。**

路由域认证是将认证密码封装在 L2 区域的 IS-IS 报文中，只有通过认证的报文才会被接收。因此，**当需要对 L2 区域进行认证时，需要对 L2 区域所有 IS-IS 设备（包括 L2 设备和 L1/2 设备）配置 IS-IS 路由域认证。**

注意 在配置 IS-IS 认证时，**要求同一区域或路由域的所有设备的认证方式和密码都必须一致，**只有这样 IS-IS 报文才会正常扩散。但无论是否通过区域认证或者路由域认证，均不影响 L1 或者 L2 邻居关系的建立。

IS-IS 区域和路由域认证的配置步骤如表 13-14 所示（区域认证和路由域认证是并列关系，可单独配置，也可同时配置）。

表 13-14 IS-IS 区域和路由域认证的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**isis** 例如：[Huawei]**isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
3	**area-authentication-mode** { { **simple** | **md5** } { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**ip** | **osi**] |**keychain** *keychain-name* | **hmac-sha256 key-id** *key-id* } [**snp-packet**	（可选）配置区域认证模式，设置 IS-IS 区域按照预定的方式和密码认证收到的 L1 路由信息报文（LSP 和 SNP），并为发送的 L1 报文加上认证信息。它支持简单认证、MD5 认证、HMAC-SHA256 认证和 Keychain 认证 4 种模式。命令中除以下选项外，**其他参数和选项说明参见上节表 13-13 中的对应参数和选项说明**，只不过这里是对 L1 区域的报文

（续表）

步骤	命令	说明
3	{ **authentication-avoid** | **send-only** } | **all-send-only**] 例如：[Huawei-isis-1]**area-authentication-mode md5** hello	（非 Hello 报文）进行认证 ● **snp-packet**：二选一选项，指定认证 SNP 报文 ● **authentication-avoid**：二选一选项，指定不对产生的 SNP 报文封装认证信息，也不认证收到的 SNP 报文。只对产生的 LSP 报文封装认证信息，并认证收到的 LSP 报文 ● **send-only**：二选一选项，指定对产生的 LSP 和 SNP 报文封装认证信息，只认证收到的 LSP 报文，不认证收到的 SNP 报文 ● **all-send-only**：二选一选项，指定仅对产生的 LSP 和 SNP 报文封装认证信息，不认证收到的 LSP 和 SNP 报文 缺省情况下，系统不对产生的 L1 路由信息报文封装认证信息，也不认证收到的 L1 路由信息报文，可用 **undo area-authentication-mode** 命令恢复 IS-IS 区域认证为缺省状态
4	**domain-authentication-mode** {{ **simple** | **md5** } {**plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**ip** | **osi**] | **keychain***keychain-name* | **hmac-sha256 key-id** *key-id* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**] 例如：[Huawei-isis-1] **domain-authentication-mode simple** huawei	（可选）设置 IS-IS 路由域中按照预设的方式和密码认证收到的 L2 路由信息报文，并在发送的 L2 区域报文中添加认证信息。命令中的参数和选项**参见本表第 3 步区域认证的对应参数和选项说明**，只不过这里是对 L2 区域的报文（非 Hello 报文）进行认证 缺省情况下，系统不对产生的 L2 路由信息报文封装认证信息，也不会认证收到的 L2 路由信息报文，可用 **undo domain-authentication-mode** 命令恢复路由域认证为缺省状态

说明 以上 IS-IS 区域认证和路由域认证支持以下几种组合形式。

① 对发送的 LSP 和 SNP 报文都封装认证信息，并认证收到的 LSP 和 SNP 报文是否通过认证，丢弃没有通过认证的报文。该情况下不能选择 **snp-packet** 或 **all-send-only** 选项。

② 仅对发送的 LSP 报文封装认证信息，并认证收到的 LSP 报文，不对发送的 SNP 报文封装认证信息，也不认证收到的 SNP 报文。该情况下能选择 **snp-packet authentication-avoid** 选项。

③ 对发送的 LSP 和 SNP 报文都封装认证信息，仅认证收到的 LSP 报文，不认证收到的 SNP 报文。这种情况下需要选择 **snp-packet send-only** 选项。

④ 对发送的 LSP 和 SNP 报文都封装认证信息，但对收到的 LSP 和 SNP 报文都不认证。这种情况下需要选择 **all-send-only** 选项。

13.10 配置 IS-IS 与 BFD 联动

可以通过配置 IS-IS Auto FRR（在此不作介绍）、IS-IS 与 BFD 联动和 IS-IS GR（在

此不作介绍）提高 IS-IS 路由的可靠性。在配置 IS-IS 可靠性之前，也需要配置 IS-IS 的基本功能。

说明 目前，BFD 会话不会感知路由切换。如果绑定的对端 IP 地址改变引起路由切换到其他链路上，除非原链路转发不通，否则，BFD 不会重新协商。且由于 IS-IS 只能建立单跳邻居，所以 IS-IS **与 BFD 联动只对 IS-IS 邻居间的单跳链路进行检测。**

13.10.1 配置 IS-IS 与静态 BFD 联动

在 IS-IS 网络中，IS-IS 邻居之间通过定时发送 Hello 报文来感知邻居状态变化，缺省情况下当发送 3 个无效的 Hello 报文（30 s）之后，即认为邻居变为 Down 状态。而这个感知速度对于一些对网络收敛速度要求较高且不能容忍丢包的网络来说是不可接受的。

为了解决上述问题，IS-IS 协议引入了 IS-IS 与 BFD 联动功能。因为 BFD 检测是毫秒级的，可以在 50 ms 内感知 IS-IS 邻居之间链路的故障，因此可以大幅度提高 IS-IS 路由的收敛速度，保障链路快速切换，减少流量损失。

如图 13-23 所示，各路由器上使能 IS-IS 基本功能。在 RouterA 和 RouterD 上使能 IS-IS 与 BFD 联动检测机制，就可实现当主路径上的链路出现故障时，BFD 能够快速检测到故障并通告给 IS-IS 协议。同时，IS-IS Down 掉故障链路的接口邻居并删除邻接对应的 IP 路由，从而触发拓扑计算，同时更新 LSP 使得其他邻居（如 RouterC）及时收到 RouterB 的更新 LSP，实现了网络拓扑的快速收敛。

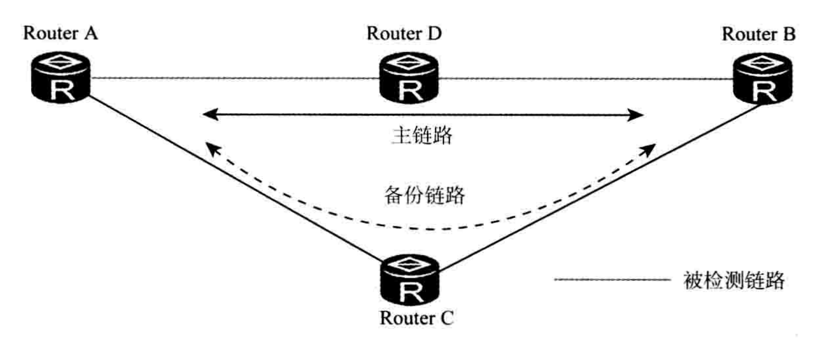


图 13-23 IS-IS 与 BFD 联动示意图

IS-IS 既可以与动态 BFD 联动，又可以与静态 BFD 联动。静态 BFD 的优点是可以人为控制，部署比较灵活，为了节省内存，同时又保证关键链路的可靠性，可以在某些指定链路部署 BFD，而其他链路不部署；静态 BFD 的缺点在于建立和删除 BFD 会话时都需要手动触发，缺乏灵活性，而且有可能造成人为的配置错误。例如，如果配置了错误的本地标识符或者远端标识符，BFD 会话将不能正常工作。

IS-IS 与静态 BFD 联动的配置步骤如表 13-15 所示（**需要在 BFD 检测的主链路两端的设备上分别配置**）。

表 13-15 **IS-IS 与静态 BFD 联动的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	**bfd** *session-name* **bind peer-ip** *ip-address* [**interface** *interface-type interface-number*] 例如：[Huawei] **bfd** test **bind peer-ip** 1.1.1.2 **interface** gigabitethernet **1/0/0.1**	创建 BFD 绑定。指定对端 IP 和本端接口，表示检测单跳链路，即检测以该接口为出接口、以 **peer-ip** 为下一跳地址的一条固定路由，并进入 BFD 会话视图。命令中的参数说明如下 • *session-name*：指定 BFD 会话的名称，1～15 个字符，不支持空格 • **peer-ip** *ip-address*：指定 BFD 会话绑定的对端 IP 地址 • **interface** *interface-type interface-number*：可选参数，指定绑定 BFD 会话的本端接口类型和接口编号。**单跳检测必须绑定对端 IP 地址和本端相应接口，多跳检测只需绑定对端 IP 地址** 【说明】在第一次创建单跳 BFD 会话时，必须绑定对端 IP 地址和本端相应接口，且创建后不可修改。如果需要修改，则只能删除后重新创建。在创建 BFD 配置项时，系统只检查 IP 地址是否符合 IP 地址格式，不检查其正确性，但绑定错误的对端 IP 地址或源 IP 地址都将导致 BFD 会话无法建立 目前，BFD 会话不会感知路由切换，所以如果绑定的对端 IP 地址改变引起路由切换到其他链路上，除非原链路转发不通，否则 BFD 不会重新协商 缺省情况下，未创建 BFD 会话绑定，可用 **undo bfd** *session-name* 命令删除指定的 BFD 会话，同时取消对应 BFD 会话的绑定信息
5	**discriminator local** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator local** 80	配置 BFD 会话的本地标识符，标识符用来区分两个系统之间的多个 BFD 会话，取值范围为 1～8 191 的整数 【注意】配置标识符时，**本端的本地标识符与对端的远端标识符必须相同，否则 BFD 会话无法正确建立，并且本地标识符和远端标识符配置成功后不可修改。对于使用缺省组播 IP 地址的 BFD 会话，本地标识符和远端标识符不能相同（其他情况下可以相同）** 静态 BFD 会话的本地标识符和远端标识符配置成功后，不可以修改。如果需要修改静态 BFD 会话本地标识符或者远端标识符，则必须先删除该 BFD 会话，然后配置本地标识符或者远端标识符
6	**discriminator remote** *discr-value* 例如：[Huawei-bfd-session-test] **discriminator remote** 80	配置 BFD 会话的远端标识符，标识符用来区分两个系统之间的多个 BFD 会话，取值范围为 1～8 191 的整数 其他注意事项参见上一步的 **discriminator local** *discr-value* 命令
7	**commit** 例如：[Huawei-bfd-session-test] **commit**	提交 BFD 会话配置。**无论改变任何 BFD 配置，必须执行本命令后才能使配置生效**

（续表）

步骤	命令	说明
8	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要绑定 BFD 会话的 IS-IS 接口，进入接口视图。该接口必须事先已使能了 IS-IS 功能
9	**isis bfd static** 例如：[Huawei-GigabitEthernet1/0/0]**isis bfd static**	使能指定 IS-IS 接口的静态 BFD 特性 缺省情况下，IS-IS 接口未使能静态 BFD 特性，可用 **undo isis bfd static** 命令去使能指定 IS-IS 接口的静态 BFD 特性

配置好后，可以通过执行 **display isis** [*process-id* | **vpn-instance** *vpn-instance-name*] **bfd session** { **peer** *ip-address* | **all** }命令查看 BFD 会话信息；也可以通过执行 **display isis interface verbose** 命令看到 IS-IS 进程的静态 BFD 的状态为 Yes。

13.10.2 配置 IS-IS 与动态 BFD 联动

IS-IS 与动态 BFD 联动由 IS-IS 协议动态触发建立 BFD 会话，即 IS-IS 在建立邻居关系时将邻居的参数及检测参数（包括目的地址、源地址等）通告给 BFD，BFD 会根据收到的参数建立起会话。当 BFD 检测到故障的时候，通过路由管理通知 IS-IS。IS-IS 进行相应邻居 Down 处理，快速发布变化的 LSP 信息和进行增量路由计算，从而实现路由的快速收敛。

动态 BFD 由路由协议动态触发 BFD 会话建立，避免了人为控制可能导致的配置错误，且配置比较简单，适用在全网需要配置 BFD 的情况。

IS-IS 与动态 BFD 的联动可以在 IS-IS 进程下全局配置，也可以在接口上具体配置，还可以同时配置，但接口下的配置优先级高于进程中的配置。这两种 IS-IS 与动态 BFD 联动的配置方法的具体配置步骤如表 13-16 所示（**需要在 BFD 检测的主链路两端的设备上分别配置**）。

表 13-16　　IS-IS 与动态 BFD 联动的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 功能，并进入 BFD 视图
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	**isis** *process-id* 例如：[Huawei] **isis**	启动对应的 IS-IS 进程，进入 IS-IS 视图
5	**bfd all-interfaces enable** 例如：[Huawei-isis-1] **bfd all-interfaces enable**	在 IS-IS 进程下使能所有的 IS-IS 接口的 BFD 特性。配置此命令会为所有 IS-IS 接口使用缺省的 BFD 参数值建立 BFD 会话 缺省情况下，IS-IS 进程下未使能 BFD 特性，可用 **undo bfd all-interfaces enable** 命令去使能 IS-IS 进程下的 BFD 特性

（续表）

步骤	命令	说明
方式 1：在 IS-IS 进程下全局配置 IS-IS 与 BFD 联动		
6	**bfd all-interfaces** { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } * 例如：[Huawei-isis-1] **bfd all-interfaces min-tx-interval** 600	（可选）指定用于建立 BFD 会话的各个参数值。执行该命令后，所有 IS-IS 接口建立 BFD 会话的参数都会改变。命令中的参数和选项说明如下 ● **min-rx-interval** *receive-interval*：可多选参数，指定期望从对端接收 BFD 报文的最小接收间隔，取值范围为 10～2 000 的整数毫秒。BFD 报文的接收间隔直接决定了 BFD 会话的检测时间。对于不太稳定的链路，如果配置的 BFD 报文的接收间隔较小，则 BFD 会话可能会发生振荡，这时可以选择增大 BFD 报文的接收间隔 ● **min-tx-interval** *transmit-interval*：可多选参数，指定向对端发送 BFD 报文的最小发送间隔，取值范围为 10～2 000 的整数毫秒。BFD 报文的发送间隔也直接决定了 BFD 会话的检测时间。对于比较稳定的链路，由于不需要频繁地检测链路状态，因此可以增大 BFD 报文的发送间隔 ● **detect-multiplier** *multiplier-value*：可多选参数，指定本地检测倍数，取值范围为 3～50 的整数，缺省值是 3。对于比较稳定的链路，由于不需要频繁地检测链路状态，因此可以增大 BFD 会话的检测倍数 ● **frr-binding**：可多选选项，指定将 BFD 会话状态与 IS-IS Auto FRR 进行绑定。BFD 检测到接口链路故障后，BFD 会话状态会变为 Down 并触发系统进行快速重路由，将流量从故障链路切换到备份链路上，从而达到流量保护的目的。但 AR150/160/200 系列不支持该选项 【说明】本端的 **min-rx-interval** 配置值与对端的 **min-tx-interval** 配置值协商得到最终的 *receive-interval* 参数值，如果在 *receive-interval*×*multiplier-value* 时间间隔内没有收到对方发送的 BFD 报文，就宣告邻居失效 缺省情况下，BFD 会话参数的值均为缺省值，即 *receive-interval* 和 *transmit-interval* 为 1 000 ms，*multiplier-value* 为 3 倍，可用 **undo bfd all-interfaces** { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } *命令恢复 BFD 会话参数为缺省值
7	**quit** 例如：[Huawei-isis-1] **quit**	退出 IS-IS 视图，返回系统视图
8	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 1/0/0	键入要禁止 BFD 特性的 IS-IS 接口，进入接口视图
9	**isis bfd block** 例如：[Huawei-GigabitEthernet1/0/0]**isis bfd block**	（可选）阻止 IS-IS 接口动态创建 BFD 会话的功能，对不需要使能 BFD 特性的 IS-IS 接口取消 BFD 特性 缺省情况下，不阻止 IS-IS 接口动态创建 BFD 会话的功能，**undo isis bfd block** 命令用来恢复为缺省状态
方式 2：在指定接口下配置 IS-IS 与动态 BFD 联动		
6	**quit** 例如：[Huawei-isis-1] **quit**	退出 IS-IS 视图，返回系统视图

（续表）

步骤	命令	说明
7	**interface** *interface-type interface-number* 例如：[Huawei] **interface** gigabitethernet 2/0/0	键入要使能 BFD 会话特性的 IS-IS 接口，进入接口视图。必须已使能 IS-IS 功能的接口
8	**isis bfd enable** 例如：[Huawei-GigabitEthernet2/0/0] **isis bfd enable**	使能以上 IS-IS 接口的 BFD 特性 【注意】必须先在前面第 5 步中使能全局 BFD，否则接口上的 BFD 参数可以配置，但不会创建 BFD 会话 当配置了全局 BFD 特性，没有配置下一步的接口 BFD 会话参数，且该接口的邻居状态为 Up（广播网中 DIS Up）时，则该接口使用缺省的 BFD 参数值建立 BFD 会话 缺省情况下，IS-IS 接口未使能 BFD 特性，可用 **undo isis bfd enable** 命令去使能指定 IS-IS 接口的 BFD 特性
9	**isis bfd** { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } * 例如：[Huawei-GigabitEthernet2/0/0] **isis bfd min-rx-interval** 600 **detect-multiplier** 4	在指定 IS-IS 接口上配置 BFD 会话的参数值。命令中的参数和选项说明参见本表前面介绍的在IS-IS进程下配置中第 6 步 **bfd all-interfaces** 命令的说明 【说明】接口配置的 BFD 特性优先级高于进程配置的 BFD 特性优先级。如果打开了接口的 BFD 开关，则按照接口上 BFD 参数建立 BFD 会话 缺省情况下，BFD 会话参数的值均为缺省值，即 *receive-interval* 和 *transmit-interval* 为 1 000 ms，*multiplier-value* 为 3 倍，可用 **undo isis bfd** { **min-rx-interval** [*receive- interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier**[*multiplier-value*] | **frr-binding** } *命令恢复以上 IS-IS 接口上 BFD 会话参数为缺省值

当链路两端均使能 BFD 特性后，执行 **display isis** [*process-id* | **vpn-instance** *vpn-instance-name*] **bfd session** { **all** | **peer** *ip-address* | **interface***interface-type interface-number* } 命令，可以查看到 BFD 的状态为 Up。

13.10.3 IS-IS 与静态 BFD 联动配置示例

本示例的基本拓扑结构如图 13-24 所示，现网中有三台路由器通过 IS-IS 协议实现路由互通，且 RouterA 与 RouterB 之间通过一台二层交换机实现互连。现要求当 RouterA 与 RouterB 之间出现链路故障时，这两台路由器能快速对故障结果做出反应，重新建立邻居关系。

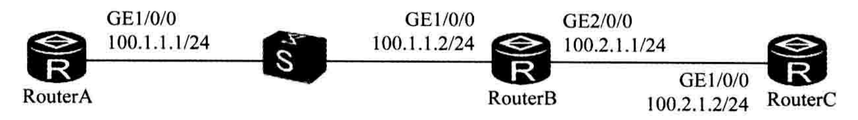


图 13-24 IS-IS 与静态 BFD 联动配置示例拓扑结构

1. 基本配置思路分析

由于本示例中 RouterA 和 RouterC 之间中间隔了一个 RouterB，所以不建立 IS-IS 邻居，不能通过 IS-IS 与 BFD 的联动检测 RouterA 到 RouterC 之间的多跳链路（**因为 IS-IS 只能建立单跳邻居关系**），只能在 RouterA 和 RouterB 之间检测单跳链路。所涉及的配置

任务如下。

① 配置各路由器的接口 IP 地址以及 IS-IS 路由协议，实现路由器之间路由可达。

② 配置各路由器的基本 IS-IS 功能。

③ 在 RouterA 和 RouterB 上分别配置 IS-IS 与静态 BFD 联动，使得双方设备可以快速感知它们之间链路的故障状态变化。

2. 具体配置步骤

① 配置各路由器的接口 IP 地址。现仅以 RouterA 上的接口 IP 地址配置为例进行介绍，RouterB、RouterC 上的接口 IP 地址配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 100.1.1.1 24
```

② 配置各路由器的 IS-IS 基本功能，包括创建 IS-IS 进程，配置路由器类型（均为 L2 类型）、网络实体名称，以及在接口上使能 IS-IS 功能。三台路由器的区域 ID 分别配置为 1111.1111.1111、2222.2222.2222、3333.3333.3333，同处一个骨干区域 aa 中。

RouterA 上的配置如下。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-2
[RouterA-isis-1] network-entity aa.1111.1111.1111.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-2
[RouterB-isis-1] network-entity aa.2222.2222.2222.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis enable 1
[RouterB-GigabitEthernet2/0/0] quit
```

RouterC 上的配置如下。

```
[RouterC] isis 1
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity aa.3333.3333.3333.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
```

配置好后，可以在 RouterA 上执行 **display isis peer** 命令，即可看到 RouterA 与 RouterB 建立了邻居关系。

```
[RouterA] display isis peer
                          Peer information for ISIS(1)
                          ----------------------------
  System Id       Interface          Circuit Id            State   HoldTime Type    PRI
2222.2222.2222 GE1/0/0           2222.2222.2222.00          Up       23s      L2       64
```

也可在 RouterA 上通过执行 **display isis route** 命令查看到其 IS-IS 路由表中有去往

RouterB 和 RouterC 的路由表项。表明以上各路由器的基本 IS-IS 功能配置是成功的。

```
[RouterA] display isis route
                         Route information for ISIS(1)
                         -----------------------------
                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------
 IPV4 Destination    IntCost   ExtCost   ExitInterface    NextHop     Flags
--------------------------------------------------------------------------
 100.1.1.0/24         10        NULL      GE1/0/0          Direct      D/-/L/-
 100.2.1.0/24         20        NULL      GE1/0/0          100.1.1.2   A/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                          U-Up/Down Bit Set
```

③ 在 RouterA 和 RouterB 上分别使能 BFD 特性，配置 BFD 会话。

RouterA 上的配置如下。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 100.1.1.2 interface gigabitethernet 1/0/0
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis bfd static
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip 100.1.1.1 interface gigabitethernet 1/0/0
[RouterB-bfd-session-btoa] discriminator local 2
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis bfd static
[RouterB-GigabitEthernet1/0/0] quit
```

配置好后，通过在 RouterA 或 RouterB 上执行 **display bfd session** 命令可以看到它们之间的 BFD 会话的状态为 Up。以下是 RouterA 上的输出示例。

```
[RouterA] display bfd session all
--------------------------------------------------------------------------
 Local Remote PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------
 1       2      100.1.1.2       Up       S_IP_IF     GE1/0/0
--------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

在 RouterA 上打开终端显示信息中心发送的日志信息功能。

```
<RouterA> terminal logging
<RouterA> terminal monitor
```

对 RouterB 的 GigabitEthernet1/0/0 接口执行 **shutdown** 命令，模拟链路故障。此时就可以在 RouterA 连接的终端上看到以下日志信息和调试信息，表明 IS-IS 根据 BFD 报告的故障删除了与 RouterB 的邻居关系。

```
ISIS/4/PEER_DOWN_BFDDOWN/1880166931 UL/R "ISIS 1 neighbor
2222.2222.2222 was Down on interface GE1/0/0
because the BFD node was down. The Hello packet was received at 11:32:10 last
time; the maximum interval for sending Hello packets was 9247;the local router sent 426 Hello
 packets and received 61 packets;the type of the Hello packet was Lan Level-2."
```

在 RouterA 上执行 **display isis route** 或 **display isis peer** 命令，不显示任何信息，表明 RouterA 与 RouterB 之间的 IS-IS 邻居关系已经拆除。

13.10.4 IS-IS 与动态 BFD 联动配置示例

本示例的基本拓扑结构如图 13-25 所示，在网络中有三台路由器通过 IS-IS 协议实现路由互通，且 RouterA 与 RouterB 之间通过一台二层交换机实现互连。现要求当 RouterA 与 RouterB 之间经交换机的链路出现故障时，这两台路由器能快速对故障结果做出反应，并把流量切换至经 RouterC 链路转发。

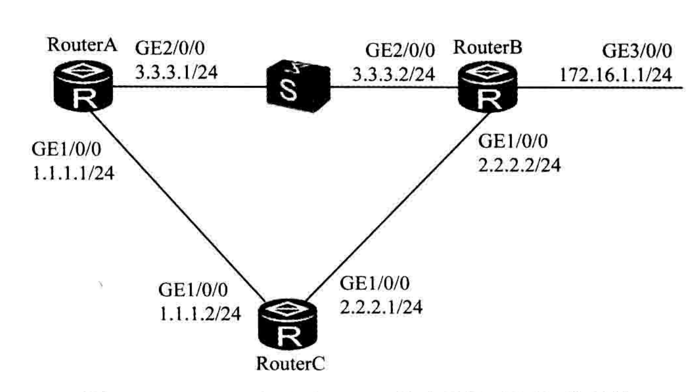


图 13-25 IS-IS 与动态 BFD 联动配置示例拓扑结构

1. 基本配置思路分析

本示例采用的是 IS-IS 与动态 BFD 联动特性，要实现主备链路切换，这就涉及主备路由的问题。因为本示例中各路由器接口均为 GE 接口，所以这些接口缺省的开销均为 20（参见 13.6.2 小节的表 13-6）。

为了实现主备路由功能，可以通过配置 IS-IS 接口开销值控制路由的选路功能，使得 RouterA 到 RouterB 经交换机的链路为主链路，经 RouterC 的链路为备份链路。然后在 RouterA、RouterB 和 RouterC 上配置 IS-IS 与动态 BFD 联动，实现快速感知链路故障，从而将流量切换至备份链路转发。当然，同样在此之前要配置各路由器的接口 IP 地址以及 IS-IS 基本功能，实现路由器之间路由可达。

2. 具体配置步骤

① 配置各路由器的接口 IP 地址。现仅以 RouterA 上的接口 IP 地址配置为例进行介绍，RouterB、RouterC 上的接口 IP 地址配置方法一样，略。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 24
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet1/0/0] ip address 3.3.3.1 24
```

② 配置各路由器的 IS-IS 基本功能，包括创建 IS-IS 进程，配置路由器类型（均为

L2 类型）、网络实体名称以及在接口上使能 IS-IS 功能。三台路由器的区域 ID 分别配置为 0000.0000.0001、0000.0000.0002、0000.0000.0003，同处一个骨干区域 10 中。

RouterA 上的配置如下。

```
[RouterA] isis
[RouterA-isis-1] is-level level-2
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] isis
[RouterB-isis-1] is-level level-2
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] isis enable 1
[RouterB-GigabitEthernet3/0/0] quit
```

RouterC 上的配置如下。

```
[RouterC] isis
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitEthernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable 1
[RouterC-GigabitEthernet2/0/0] quit
```

配置好后，可以使用 **display isis peer** 命令查看到 RouterA 和 RouterB、RouterA 和 RouterC 已建立了邻居关系。以下为 RouterA 的输出示例。

```
[RouterA] display isis peer
                          Peer information for ISIS(1)
                          ----------------------------
  System Id       Interface        Circuit Id              State HoldTime    Type    PRI
0000.0000.0002   GE2/0/0           0000.0000.0002.01 Up    9s                L2      64
0000.0000.0003   GE1/0/0           0000.0000.0001.02 Up    21s               L2      64
Total Peer(s): 2
```

通过执行 **display ip routing-table** 命令也可以查看到三台路由器之间已经互相学习到路由。以下同样是 RouterA 上的输出示例。从路由表可以看出，到达 172.16.1.0/24 的路由下一跳地址为 3.3.3.2（RouterB 的 GE2/0/0 接口 IP 地址），流量在主链路 RouterA→RouterB 上传输（**参见输出信息中的粗体字部分**）。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8          Routes : 9
Destination/Mask    Proto   Pre  Cost       Flags  NextHop        Interface
        1.1.1.0/24  Direct  0    0            D    1.1.1.1        GigabitEthernet1/0/0
        1.1.1.1/32  Direct  0    0            D    127.0.0.1      InLoopBack0
        1.1.1.1/32  Direct  0    0            D    127.0.0.1      GigabitEthernet1/0/0
        2.2.2.0/24  ISIS-L2 15   20           D    1.1.1.2        GigabitEthernet1/0/0
        3.3.3.0/24  Direct  0    0            D    3.3.3.1        GigabitEthernet2/0/0
        3.3.3.1/32  Direct  0    0            D    127.0.0.1      InLoopBack0
        3.3.3.1/32  Direct  0    0            D    127.0.0.1      GigabitEthernet2/0/0
      127.0.0.0/8   Direct  0    0            D    127.0.0.1      InLoopBack0
      127.0.0.1/32  Direct  0    0            D    127.0.0.1      InLoopBack0
      172.16.1.0/24 ISIS-L2 15   20           D    3.3.3.2        GigabitEthernet2/0/0
```

③ 配置接口开销值，把 RouterA 和 RouterB 的 GE2/0/0 的开销值改为比缺省值 20 更小的 5，为的就是以便在主链路故障恢复后，流量自动切换到主链路上。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet1/0/0] isis cost 5
[RouterA-GigabitEthernet1/0/0] quit

[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet1/0/0] isis cost 5
[RouterB-GigabitEthernet1/0/0] quit
```

④ 在 RouterA 和 RouterB 上分别使能 IS-IS 进程下的 BFD 特性。

RouterA 上的配置如下。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] isis
[RouterA-isis-1] bfd all-interfaces enable
[RouterA-isis-1] quit
```

RouterB 上的配置如下。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] isis
[RouterB-isis-1] bfd all-interfaces enable
[RouterB-isis-1] quit
```

⑤ 分别在 RouterA 和 RouterB 上的 GE2/0/0 接口上使能 BFD 特性，并指定最小发送和接收间隔为 100 ms，本地检测时间倍数为 4。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis bfd enable
[RouterA-GigabitEthernet2/0/0] isis bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
[RouterA-GigabitEthernet2/0/0] quit

[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis bfd enable
[RouterB-GigabitEthernet2/0/0] isis bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
[RouterB-GigabitEthernet2/0/0] quit
```

配置好后，在 RouterA 或 RouterB 上执行 **display isis bfd session all** 命令便可以查看到 BFD 参数已生效，并且 BFD 会话状态为 Up。以下是 RouterB 上的输出示例。

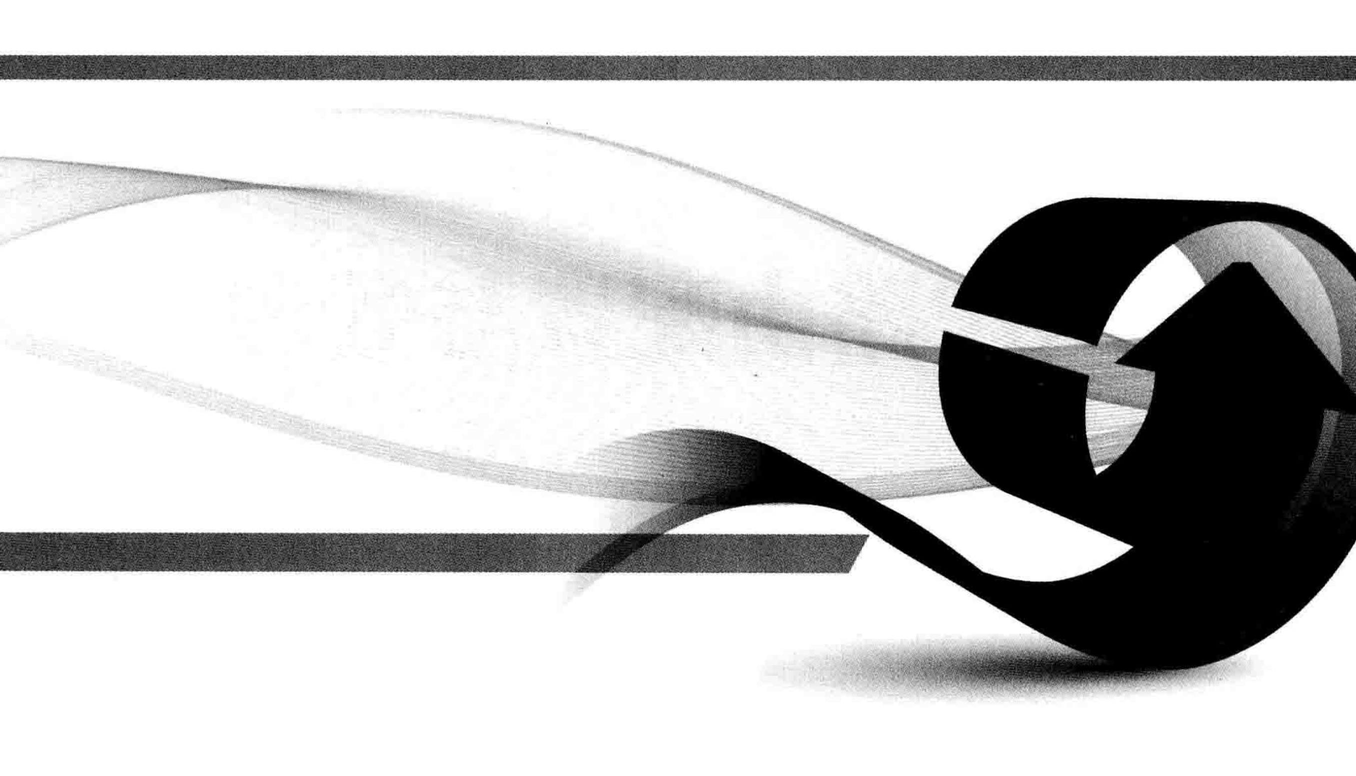
```
[RouterB] display isis bfd session all
                        BFD session information for ISIS(1)
                        ------------------------------------
Peer System ID : 0000.0000.0001           Interface : GE2/0/0
TX : 100              BFD State : up           Peer IP Address : 3.3.3.1
RX : 100              LocDis : 8192            Local IP Address: 3.3.3.2
Multiplier : 4        RemDis : 8192        Type : L2
Diag : No diagnostic information
```

现对 RouterB 的 GigabitEthernet2/0/0 接口执行 **shutdown** 命令，模拟主链路故障。此时查看 RouterA 上的 IP 路由表，可以看出，到达 172.16.1.0/24 的路由下一跳地址为 1.1.1.2（RouterC 的 GE1/0/0 接口 IP 地址），流量在主链路 RouterA→RouterC→RouterB 上传输（**参见输出信息中的粗体字部分**）。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8          Routes : 8
Destination/Mask    Proto     Pre  Cost        Flags NextHop         Interface
        1.1.1.0/24  Direct    0    0             D   1.1.1.1         GigabitEthernet1/0/0
        1.1.1.1/32  Direct    0    0             D   127.0.0.1       InLoopBack0
        1.1.1.1/32  Direct    0    0             D   127.0.0.1       GigabitEthernet1/0/0
        2.2.2.0/24  ISIS-L2   15   20            D   1.1.1.2         GigabitEthernet1/0/0
        3.3.3.0/24  Direct    0    0             D   3.3.3.1         GigabitEthernet1/0/0
        3.3.3.1/32  Direct    0    0             D   127.0.0.1       InLoopBack0
        3.3.3.1/32  Direct    0    0             D   127.0.0.1       GigabitEthernet1/0/0
      127.0.0.0/8   Direct    0    0             D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct    0    0             D   127.0.0.1       InLoopBack0
    172.16.1.0/24   ISIS-L2 15     40            D   1.1.1.2         GigabitEthernet1/0/0
```

【经验之谈】在备份链路中的 IS-IS 路由开销为 RouterA 的 GE1/0/0 接口和 RouterB 的 GE1/0/0 接口所在链路之和，所以该 IS-IS 路由开销为 40（两接口缺省开销均为 20）。

当主链路恢复正常后，到达 172.16.1.0/24 的路由又将恢复为主链路，因为此时主链路的路由开销为 5，低于备份链路的路由开销 40，优先级更高。



第14章
BGP路由配置与管理



BGP是个复杂而又庞大的距离矢量类型动态路由协议，其中涉及许多非常复杂的配置。与前面介绍的RIP、OSPF、IS-IS路由协议属于内部网关协议（IGP）不同，BGP路由协议属于外部网关协议（EGP）。另外，BGP本身不产生路由，而是通过引入其他类型的路由在对等体中间传播的。正因如此，BGP路由协议中解决的不再是同一AS不同路由器之间的选路问题，而是解决不同AS之间的选路问题（也可在同一AS内部路由器上运行，称之为IBGP），这也正是BGP路由协议广泛应用于广域网的根本原因。

与学习其他动态路由协议类似，学习BGP协议的关键是要理解各种报文的功能及格式、BGP对等体建立、各种BGP路由属性、BGP的选路规则、BGP路由聚合、BGP认证、BGP负载分担以及像BGP的路由引入、BGP路由信息的接收和发布控制、调整BGP网络收敛速度、简化IBGP网络连接的路由反射器和联盟技术等。本章将对以上各项基础知识、工作原理以及各种功能的配置与管理方法进行详细介绍，并同时列举大量实际配置案例，以加深读者对基础知识、工作原理和配置方法的理解。

14.1 BGP 基础

BGP（Border Gateway Protocol，边界网关协议）是一种实现 AS（自治系统）之间路由的距离矢量性动态路由协议。它不同于本书前面各章介绍的 RIP、OSPF 和 IS-IS 协议，它们均是用于解决一个 AS 内部网络路由的 IGP（内部网关协议），而 BGP 则是用于解决不同 AS 间网络路由的 EGP（Exterior Gateway Protocol，外部网关协议）。

14.1.1 BGP 简介

为方便管理规模不断扩大的网络，网络被分成了不同的自治系统。1982 年，EGP 被用于在 AS 之间动态交换路由信息。但是 EGP 设计得比较简单，只发布网络可达的路由信息，而不对路由信息进行优选，同时也没有考虑环路避免等问题，所以很快就无法满足网络管理的要求。

BGP 是用于取代最初的 EGP 而设计的另一种外部网关协议。与最初的 EGP 不同，BGP 能够进行路由优选、避免路由环路、更高效地传递路由和维护大量的路由。早期发布的 3 个版本分别是 BGP-1（RFC1105）、BGP-2（RFC1163）和 BGP-3（RFC1267）。1994 年开始使用 BGP-4（RFC1771）；2006 年之后单播 IPv4 网络使用的版本是 BGP-4（RFC4271），其他网络使用的版本是 MP-BGP（RFC4760）；再后来开发的 BGP-4+提供了对 IPv6 单播网络的支持，用于控制 IPv6 单播网络中路由的传播和选择。**本章主要就 IPv4 单播网络中使用的 BGP-4 和 IPv4 其他网络中使用的 MP-BGP 版本进行功能配置与管理介绍。**

说明 AR150/150-S/160/200/200-S/1200/1200-S/2200/2200-S/3200 系列路由器的 BGP 特性均同时支持 BGP-4、BGP-4+和 MP-BGP。**在 BGP 视图下的配置将对 BGP-4、BGP-4+和 MP-BGP 同时生效。缺省情况下，在 BGP IPv4 单播地址族视图下配置的命令也可以在 BGP 视图下直接配置，但只对 BGP4 生效**。例如，如果在 BGP 视图下配置 BGP 引入路由后，则只对 BGP-4 生效，对 BGP-4+和 MP-BGP 不生效，它们需要在对应的地址族视图下配置。

另外，虽然 BGP 用于在 AS 之间传递路由信息，但并不是所有 AS 之间传递路由信息都需要运行 BGP。在一些网络出口比较单一的 AS 边界，可以用更为简单的静态路由来配置。比如在数据中心上行连入 Internet 的出口上，为了避免 Internet 海量路由对数据中心内部网络的影响，设备采用静态路由代替 BGP 与外部网络通信。

1. BGP 中的 AS

AS 是指在一个组织机构管辖下的拥有相同选路策略的 IP 网络。BGP 网络中的每个 AS 都被分配了一个唯一的 AS 号，用于区分不同的 AS。BGP 中的 AS 号分为 2 字节 AS 号和 4 字节 AS 号，其中 2 字节 AS 号的范围为 1～65 535 的整数，4 字节 AS 号的范围为 1～4 294 967 295 的整数（可以有不同表示格式），属于扩展 AS 号。支持 4 字节 AS 号的设备能够与支持 2 字节 AS 号的设备兼容。

在 BGP AS 中不仅有两种不同长度的 AS 编号方法，而且还有不同的输入格式，同 s

时还有公网 AS 和私网 AS 之分，具体将在下节介绍。

2. BGP 分类

BGP 按照运行方式分为 EBGP（External/Exterior BGP，外部 BGP）和 IBGP（Internal BGP，内部 BGP）。这两种 BGP 在网络中运行的位置如图 14-1 所示。

① EBGP：运行于不同 AS 之间的 BGP 称为 EBGP。为了防止 AS 间产生环路，当 BGP 设备接收 EBGP 对等体发来的路由时，**会将路由信息 AS_Path 列表中带有本地 AS 号的路由丢弃**。AS_Path 列表在路由的 AS_Path 属性中，将在本章后面具体介绍。

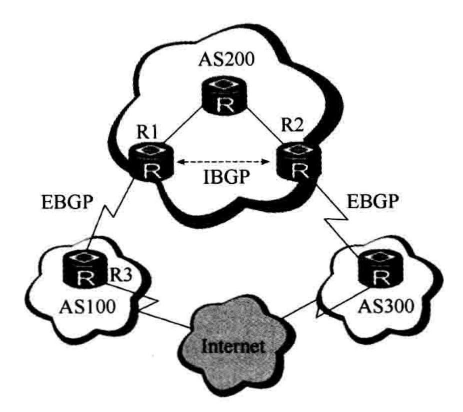


图 14-1　EBGP 和 IBGP 运行的网络位置示意图

② IBGP：运行于同一 AS 内部的 BGP 称为 IBGP。为了防止 AS 内产生环路，BGP 设备不将从 **IBGP 对等体学习到的路由发布给其他 IBGP 对等体**，并缺省需要与所有 IBGP 对等体建立全连接才能实现 AS 内部各 IBGP 设备间的路由互通。为了解决现实网络中多数情况下 AS 内部各 IBGP 设备间很难实现全连接的问题，BGP 提供了“路由反射器”和“联盟”两种解决方案。具体将在本章后面一一具体介绍。

如果在 AS 内一台 BGP 设备收到 EBGP 对等体发送的路由后，需要通过另一台 BGP 设备将该条路由信息传播给其他 AS 时，则建议将这两台 BGP 设备配置运行 IBGP。如图 14-1 所示，位于 AS200 中的 R1 收到 EBGP 对等体 R3 发送的路由后，希望把这条路由信息通过 R2 传播到 AS300 中，所以 R1 与 R2 要配置为运行 IBGP。实际上就是让它们成为 IBGP 对等体（有关“对等体”的概念将在本节后面具体介绍），由此可见 **IBGP 对等体不一定就是直接连接的**。

3. 两种 BGP 报文交互角色

BGP 报文交互中分为 Speaker 和 Peer 两种角色。

① Speaker：发送 BGP 报文的设备称为 BGP Speaker（发言者）。它接收或产生新的报文信息，并发布给其他 BGP Speaker。Speaker 角色是针对具体报文发送过程而言的，网络中每台 BGP 路由器均可成为自己发送 BGP 报文的 Speaker。

② Peer：相互交换报文的 Speaker 之间互称 Peer（对等体）。多个相关的对等体可以构成对等体组（Peer Group），然后可以为这个对等体组进行集中配置。

4. BGP 的路由器 ID（Router ID）

与 OSPF 一样，BGP 也是采用 Router ID（路由器 ID）来标识一个 BGP 设备的。路由器 ID 会在 BGP 会话建立时发送的 Open 报文中携带，也是一个 32 位值，通常是 IP 地址的形式。在对等体之间建立 BGP 会话时，每台 BGP 设备都必须有唯一的路由器 ID，否则对等体之间不能建立 BGP 连接。

在整个 BGP 网络中，每台 BGP 设备的路由器 ID 必须唯一，可以采用手动配置，也可以让 BGP 自己在设备上选取。**在没有手动配置路由器 ID 的缺省情况下，BGP 选择设备上的 Loopback 接口的 IP 地址作为 BGP 的路由器 ID**。如果设备上既没有手动配置路由器 ID，也没有配置 Loopback 接口 IP 地址，系统会优先选择设备上物理接口中最大的

IP 地址作为 BGP 的路由器 ID。**一旦选出路由器 ID，除非发生接口地址删除等事件，否则即使配置了更大的接口 IP 地址，也会保持原来的路由器 ID。**

14.1.2 BGP AS

BGP 的 AS 用于将整个外部网络划分为一个个应用本地路由策略的路由子域，这样公司通过 BGP 可以简化路由域管理和统一策略配置，因为一个 BGP 设备可以连接多个 AS。在 BGP 设备连接的每个 AS 中可以支持多种不同的路由协议，但 BGP 本身不产生路由，需要通过引入各种 IGP 路由、直连路由和静态路由来实现与各个子网络的连接。不同的 BGP AS 中的 BGP 路由器间需通过 EBGP 对等会话动态交换路由信息；同一个 AS 内部的 BGP 路由器间通过 IBGP 对等会话交换路由信息。

又因为 BGP 主要用于基于 Internet 这样的公网连接，所以它的 AS 又与仅应用于公司内部网络的 AS 不一样，在公网中使用的 AS（称之为“公用 AS”）必须在是公网注册，并由 ISP 统一分配，且在整个 Internet 中都是唯一的，就像公网 IP 地址一样。

RFC 5398 中规定，在 1～64 511 之间的 2 字节 AS 号是公网 AS，64 512～65 534 之间的 2 字节 AS 号是私网 AS（AS 号 65535 是保留用于特定用途的）。私有 AS 号可以用于内部路由域，但不能传输到达 Internet 的通信，不要配置通告私有 AS 号到外部网络。

图 14-2 举例说明了在分隔 AS 中的两个路由器可以通过 EBGP 协议进行连接。Router A 和 Router B 是两个使用公用 AS 号的独立路由子域上的 ISP 路由器。这两个路由器通过 Internet 来传输通信。Router A 和 Router B 是通过 EBGP 对等会话进行连接的。每个直接连接 Internet 的公用 AS 各自分配一个由 ISP 提供的唯一 AS 号，用于标识 BGP 进程和 AS。

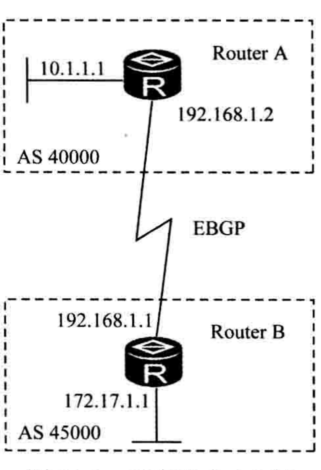


图 14-2 带有两个 AS 的简单 BGP 拓扑示例

1. BGP AS 号格式

在 2009 年 1 月之前，RFC 4271 BGP-4 中使用的 AS 号是一个 2 字节数，取值在 1～65 535 范围之间。为了满足日益增加的 AS 号需求，IANA 从 2009 年 1 月开始在 RFC 5396 中定义了 4 字节的 AS 号，取值范围从 65 536 到 4 294 967 295。AS 有以下两种表示格式。

（1）Asplain AS（无格式 AS）

Asplain AS 号格式是一个普通的十进制整数，可以是 2 字节的，也可以是 4 字节的，不同长度仅代表 AS 编号的取值范围不同，是 BGP 缺省的 AS 号格式。如 65 526 是一个 2 字节的 AS 号，而 234 567 是一个 4 字节的 AS 号。

（2）Asdot AS（点分 AS）

Asdot 格式 AS 号是一个点分记数法所表示的十进制数。它规定：如果是 2 字节的 AS 号（最大值为 65 535），则直接用它的十进制整数表示；如果是 4 字节的 AS 号，则要采用点分计数法表示。点分计数法的计算方法是先把这个十进制 AS 号转换成二进制，然后**从右向左**每 16 位（2 字节）分成一段，在两段之间以小圆点分隔，再将这两段分别换算成十进制。

例如 65 526 是一个 2 字节的 AS 号，仍采用 65 526 表示，而 234 567 是一个 4 字节

的 AS 号，则要表示为 3.379 59。按照前面介绍的方法，先把 234 567 十进制数转换成二进制，结果为 111001010001000111，然后从右向左每 16 位分成一段，分别得到 11 和 1001010001000111，然后在两段之间以小圆点分隔，再对这两段分别换算成十进制即为 3.379 59。

尽管可以任意使用 Asplain 格式或者 Asdot 格式 4 字节 AS 号，但在 **display** 命令的输出中，或者在正则表达式中仅显示或控制一种格式。在使用正则表达式来匹配 Asdot 格式 AS 号时，因为在 Asdot 格式 AS 中包括了一个在正则表达式中代表特殊含义的句点（.）符号，所以在句点前必须键入一个反斜杠（\），如 1\.14，以确保正则表达式不会匹配失败。

表 14-1 所示为采用缺省的 Asplain 格式时，两种不同 AS 配置格式的输出及正则表达式匹配的格式。从中可以看出，当采用 Asdot 格式输入 4 字节的 AS 号时，最终是以 Asplain 格式显示和匹配的，原来点分格式的 1.0～65 535.655 35 转换成了非点分格式的 65 536～4 294 967 295。

表 14-1　采用缺省的 Asplain 格式时，配置格式与输出及正则表达式匹配的格式比较

配置格式	display 命令输出格式及正则表达式匹配格式
Asplain 格式：2 字节：1～65 535， 4 字节：65 536～4 294 967 295	2 字节：1～65 535 4 字节：65 536～4 294 967 295
Asdot 格式：2 字节：1～65 535， 4 字节：1.0～65 535.655 35	2 字节：1～65 535 4 字节：65 536～4 294 967 295

表 14-2 所示为当强制设置为 Asdot 格式时，两种不同 AS 配置格式的输出及正则表达式匹配的格式。从中可以看出，当采用 Asplain 格式输入 4 字节的 AS 号时，最终是以 Asdot 格式显示和匹配的，原来非点分格式的 65 536～4 294 967 295 转换成了点分格式的 1.0～65 535.655 35。

表 14-2　采用 Asdot 格式时，配置格式与输出及正则表达式匹配的格式比较

配置格式	display 命令输出格式及正则表达式匹配格式
Asplain 格式：2 字节：1～65 535 4 字节：65 536～4 294 967 295	2 字节：1～65 535 4 字节：1.0～65 535.655 35
Asdot 格式：2 字节：1～65 535 4 字节：1.0～65 535.655 35	2 字节：1～65 535 4 字节：1.0～65 535.655 35

2. 保留的 AS 号

在 RFC 4893 BGP-4 标准中，支持由 2 字节 AS 向 4 字节的过渡。但在这个标准中新增了保留的 AS 号 23 456。后来又在新的 RFC 5398 标准中规定了新的保留 AS 号，它们是在 64 496～64 511 之间的 2 字节 AS 号和在 65 536～65 551 之间的 4 字节 AS 号。

14.1.3　BGP 地址族

最初的 BGP-4 标准仅支持 IPv4 网络，为了解决 BGP 对多种网络层协议的支持，IETF 对 BGP-4 进行了地址族能力扩展，形成 MP-BGP（Multi-Protocol BGP，多协议 BGP），使 BGP 能够为多种网络应用提供路由信息。在 RFC4760（Multiprotocol Extensions for BGP-4）中，定义了两个新的可选非过渡属性（“非过渡属性”就是该属性不能传递到其

他设备上，仅在本地设备上使用，具体将在 14.3 节介绍），BGP 的多种协议扩展都用到了这两个属性。

① 扩展协议可达 NLRI（MP_REACH_NLRI，属性类型 14）。

② 扩展协议不可达 NLRI（MP_UNREACH_NLRI，属性类型 15）。

这两种扩展属性适用于所有的 BGP 协议扩展。为了对不同的扩展类型进行区分，在这两种属性中都携带了 BGP 地址族（Address Family）和子地址族（Sub-Address Family）信息。所谓“地址族”就是一种网络层协议（如 TCP/IP 网络中的 IPv4、IPv6，以及 OSI 网络中的 CNLS）配置模块，简单地说就是把不同类型的网络分块进行配置。其目的就是把针对运行不同网络层协议的网络分别进行功能配置，这样配置起来就更加有条理，因为这些不同网络层协议的地址格式的应用需求或许根本不一样。

为了进一步区分同一类型网络中不同类型的网络应用（如 IPv4 和 IPv6 网络中都有单播、组播、VPN 等），又可在地址族下划分子地址族。“地址族”使用 AFI（Address Family Identifier，地址族标识符）进行标识，对应的子地址族为 SAFI（Subsequent Address Family Identifier，子序列地址族标识符）。

目前，在 IP 网络中，MP-BGP 主要包括 4 个地址族：IPv4、IPv6、L2VPN 和 VPLS 地址族。在 IP 地址族下又有 IPv4 单播、IPv4 组播、IPv4 VPN、IPv4 MPLS 和 IPv4 MDT 子地址族等，IPv6 地址族下有 IPv6 单播和 IPv6 组播子地址族等。表 14-3 列出了这些地址族对应的 AFI 和 SAFI 值。**AR150/150-S/160/200/200-S 系列不支持 BGP-VPNv4 地址族。**

表 14-3　BGP 常用地址族及子地址族

MP-BGP 协议族	AFI	SAFI
IPv4 Unicast（IPv4 单播）	1	1
IPv4 Multicast（IPv4 组播）	1	2
IPv4 Lable（IPv4 MPLS）	1	4
IPv4 VPNv4（IPv4 VPN）	1	128
IPv6 Unicast（IPv6 单播）	2	1
IPv4 MDT（IPv4 组播分布树）	1	66
IPv6 Multicast（IPv6 组播）	2	2
L2VPN（二层 VPN）	196	128
VPLS（虚拟专用局域网服务）	25	65

14.2　BGP 报文类型及格式

BGP-4 协议有 5 种报文：Open（建立）、Update（更新）、Notification（通知）、Keepalive（保持活跃）和 Route-refresh（路由刷新）。它们各自的作用将在下面各对应小节中介绍。但这些报文有相同的报头，其格式如图 14-3 所示。

各字段解释如下。

① Marker：占 16 字节，用于标明 BGP 报文边界，固定值为所有比特均为“1”，相

当于一个报文的头部标识符。

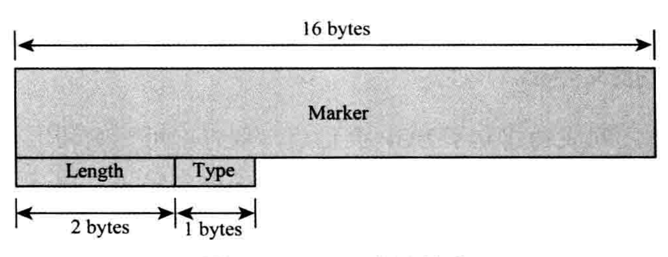


图 14-3　BGP-4 报头格式

② Length：占 2 字节，标识 BGP 报文总长度（包括报头在内），以字节为单位。

③ Type：占 1 字节，标识 BGP 报文的类型。其取值从 1 到 5，分别表示 Open、Update、Notification、Keepalive 和 Route-refresh 消息。其中，前 4 种报文是在 RFC 1771 中定义，而第 5 种报文是在 RFC 2918 中定义的。

14.2.1　Open 报文格式

Open（建立）是 TCP 连接建立后发送的第一个报文，包含本地 Speaker 信息以及用于后面与对等体间建立 TCP 会话的信息，用于建立 BGP 对等体之间的连接关系。其报文格式如图 14-4 所示。Open 报文中的各字段信息必须在对等体之间进行路由信息交换之前协商确定好。

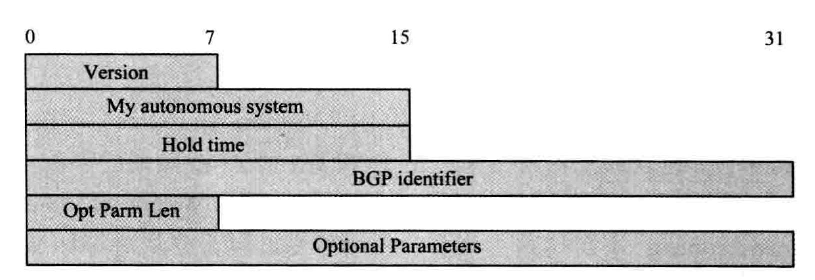


图 14-4　Open 报文格式

各字段解释如下。

① Version：标识本地设备使用的 BGP 版本，占 1 字节。对于 BGP-4 来说，其值为 4。

② My autonomous system：标识本地 AS 号，占 2 字节或 4 字节。通过比较两端的 AS 号可以确定是 EBGP 连接（不同时）还是 IBGP 连接（相同时）。

③ Hold time：标识对等体与本设备保持连接的时间，占 2 字节，以秒为单位。在建立对等体关系时两端要协商 Hold Time，并保持一致。如果在这个时间内未收到对端发来的 Keepalive 消息或 Update 消息，则认为 BGP 连接中断。

④ BGP identifier：标识 BGP 路由器的路由器 ID，占 4 字节，采用点分十进制格式的 IP 地址的形式，用来识别 BGP 路由器。

⑤ Opt Parm Len（Optional Parameters Length）：可选参数的长度，占 1 字节，标识可选参数的总长度，如果为 0 则没有可选参数。

⑥ Optional parameters：可选参数，长度可变，用于多协议扩展（Multiprotocol Extensions）等功能，如 BGP 验证信息。

14.2.2 Update 报文格式

在 BGP 对等体之间成功建立了 BGP 会话后，双方就可开始利用 Update（更新）报文进行路由信息交换了，包括要向对等体通告的每条路由信息。**但 Update 报文既可以发布可达路由信息，也可以撤销不可达路由信息**。其报文格式如图 14-5 所示。

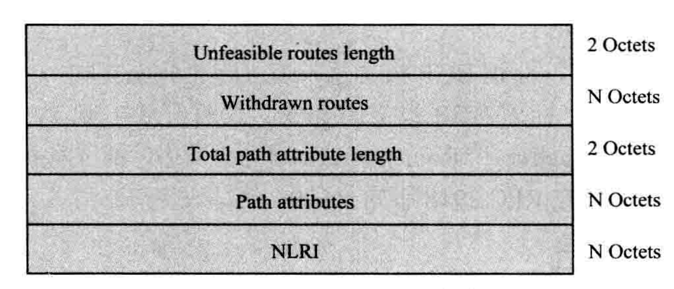


图 14-5 Update 报文格式

一条 Update 报文可以通告一类**具有相同路径属性**的可达路由，这些路由放在 NLRI（Network Layer Reachable Information，网络层可达信息）字段中，Path Attributes 字段携带了这些路由的属性，BGP 根据这些属性进行路由的选择；同时 Update 报文还可以携带多条不可达路由信息，被撤销的路由放在 Withdrawn Routes 字段中，用来通知对等体要撤销的路由。各字段解释如下。

① Unfeasible routes length：标识不可达路由（Withdrawn routes）字段的长度，占 2 字节，以字节为单位，包含通知对等体从它的 BGP 路由表中要撤销的当前不可达路由的数量。如果为 0 则说明没有要撤销的路由，也就没有下面的 Withdrawn routes 字段。

② Withdrawn routes：不可达路由列表，长度可变，包含要从对等体 BGP 路由表中撤销的当前不可达路由的网络地址及前缀。

③ Total path attribute length：标识路径属性（Path attributes）字段的长度，占 2 字节，以字节为单位。如果为 0 则说明没有下面的 Path attributes 字段。

④ Path atributes：与 NLRI 字段相关的所有路径属性列表，每个路径属性由一个 TLV（Type-Length-Value）三元组构成，可变长度。BGP 正是根据这些属性值来避免环路，进行选路、协议扩展等。

⑤ NLRI（Network Layer Reachability Information）：标识网络层可达信息，包含要向对等体通告的每条可达路由的前缀，长度可变。这些可达路由信息来自本地 Adj-RIB-In（Adjacent Routing Information Base, Incoming，入方向邻接路由信息库），然后又将加入到对端 Adj-RIB-In 中。

14.2.3 Notification 报文格式

当 BGP 检测到错误状态时，就会向对等体发出 Notification（通知）报文，之后 BGP 连接会立即中断。其报文格式如图 14-6 所示。各字段解释如下。

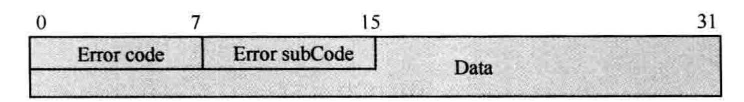


图 14-6　Notification 报文格式

① Error code：差错码，占 1 字节，指定错误类型。

② Error subcode：差错子码，占 1 字节，描述错误类型的详细信息。

③ Data：错误消息内容，可变长度，用于辅助发现错误的原因。它的内容依赖于具体的差错码和差错子码，记录的是出错部分的数据。

14.2.4　Keepalive 报文格式

BGP 会周期性地向对等体发出 Keepalive（保持活跃）报文，用来保持对等体连接的有效性。其报文格式中仅包含图 14-3 所示的 BGP 报头，没有附加其他任何字段。

14.2.5　Route-refresh 报文格式

Route-refresh（路由刷新）报文用来要求对等体重新发送指定地址族的路由信息。其报文格式如图 14-7 所示。各字段解释如下。

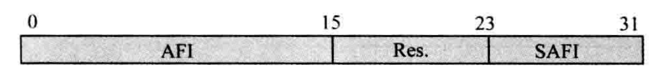


图 14-7　Route-refresh 报文格式

① AFI：Address Family Identifier，地址族标识，占 2 字节，用于标识所采用的地址族类型。不同类型地址族对应的 AFI 值参见本章前面介绍的表 14-3。

② Res.：保留，占 1 字节，必须置 0。

③ SAFI：Subsequent Address Family Identifier，子地址族标识，占 1 字节，用于标识子地址族类型。不同类型子地址族对应的 SAFI 值参见本章前面介绍的表 14-3。

14.3　BGP 的主要路由属性

BGP 路由属性是随着通过 Update 报文发送的 BGP 路由信息一起发布的一组参数。它对特定的路由进行了进一步的描述，使得路由接收者能够根据路由属性值对路由进行过滤和选择。它们可以被看作是选择路由的度量（metric）。

14.3.1　BGP 路由属性分类

BGP 路由信息包括许多属性，总体可以分成以下 4 类。

① 公认必须遵循（Well-known mandatory）：所有 BGP 设备都可以识别此类属性（这就是“公认”的含义），**且必须在 Update 报文中存在**（这就是“必须遵守”的含义），否则对应的路由信息就会出错。

② 公认任意（Well-known discretionary）：所有 BGP 设备都可以识别此类属性，但

不要求必须存在于 Update 报文中（这就是“任意”的含义），即就算缺少这类属性，路由信息也不会出错。

③ 可选过渡（Optional transitive）：BGP 设备可以不识别此类属性，如果 BGP 设备不识别此类属性，仍然会接收这类属性（这就是“可选”的含义），**且可将该属性通告给其他对等体**（这就是“过渡”的含义）。

④ 可选非过渡（Optional non-transitive）：BGP 设备可以不识别此类属性，如果 BGP 设备不识别此类属性，也会接收这类属性，**但在接收时忽略该属性，不会将该属性通告给其他对等体**（这就是“非过渡”的含义），即仅在本地路由器上使用。

常见 BGP 路由属性及所属类型如表 14-4 所示。这些属性的具体介绍将在下面各小节中进行。

表 14-4 常见 BGP 路由属性及所属类型

属性名	类型
Origin（源）属性	公认必须遵循
AS_Path（AS 路径）属性	
Next_Hop（下一跳）属性	
Local_Pref（本地优先级）属性	公认任意
Community（团体）属性	可选过渡
MED（Multi-Exit Discriminators，多出口区分）属性	可选非过渡
Originator_ID 属性	
Cluster_List 属性	

14.3.2 ORIGIN（源）属性

Origin 属性公认必须遵守（也就是所有 BGP 路由器都可识别，且必须在 Update 报文中存在）的 BGP 路由属性，用来标记一条 BGP 路由的路由信息源类型，指明了当前 BGP 路由是从哪类设备中产生的。它有以下三种类型。

① IGP(i)：是 IBGP 设备通过 **network** 命令通告的路由，是本 AS 内产生的路由，优先级最高。

② EGP(e)：是从 EGP 对等体那里学习得到的路由，优先级次之。

③ incomplete(?)：优先级最低，是通过其他方式学习到的路由信息，比如 BGP 通过 **import-route** 命令引入的外部路由。但它并不是说明路由不可达，而是表示路由的来源无法确定。

14.3.3 AS_PATH 属性

AS_Path（AS 路径）属性也是公认必须遵守的 BGP 路由属性。AS_PATH 属性按矢量（所谓“矢量”就是带有方向性的变量）顺序记录了某条路由从本地到达目的地址所经过的所有 AS 号，即“AS 路径列表”的含义。AS 路径列表可以理解为一个小括号里面包括所经过的 AS 号，各 AS 号间以逗号分隔，且离本地设备越近的 AS 编号越在前面（即小括号的左边），如（200，400，100）表示该路由经过了 AS200、AS400 和 AS100 这三个 AS，其中 AS200 离本地设备最近，AS100 离本地设备最远，也即路由的源 AS。

通过观察路由的 AS_Path 属性，BGP 设备可以找出该路由是从哪个 AS 产生的，以及该路由在传递过程中经过了多少 AS。AS 路径最右边的 AS 号就是路由的产生者（即源 AS），最左边的 AS 号就是刚刚声明该路由的那个相邻的 AS。处于 AS_Path 中间的 AS 号是路由传递经过的 AS。这样的 AS_Path 序列被称为 AS_Sequence。

当 BGP 路由器在通告路由信息时，遵循以下原则。

（1）当 BGP Speaker 通告自身引入的路由时

① 当 BGP Speaker 将这条路由发布到 EBGP 对等体时，便会在 Update 报文中创建一个携带本地 AS 号的 AS 路径列表。

② 当 BGP Speaker 将这条路由发布给 IBGP 对等体时，便会在 Update 报文中创建一个空的 AS 路径列表。

（2）当 BGP Speaker 通告从其他 BGP Speaker 的 Update 报文中学习到的路由时

① 当 BGP Speaker 将这条路由发布给 EBGP 对等体时，便会把本地 AS 编号添加在 AS 路径列表的最前面（最左面）。收到此路由的 BGP 设备根据 AS_Path 属性就可以知道去目的地址所要经过的 AS。离本地 AS 最近的相邻 AS 号排在前面，其他 AS 号按顺序依次排列。

② 当 BGP Speaker 将这条路由发布给 IBGP 对等体时，不会改变这条路由相关的 AS_Path 属性。

如图 14-8 所示，有两条从 AS 50 区域中路由器到达目的网络 8.0.0.0 的路由，根据箭头所示的路由发布方向（**路由发布方向是到达目的地址的路由路径的反方向**）可以看出，在 AS_Path 列表中依次添加了所经过的 AS 号，并且是最近的处于最前面，其他 AS 号按顺序依次排列，中间以逗号分隔。如最后 D=8.0.0.0（30，20，10）和 D=8.0.0.0（40，10）。

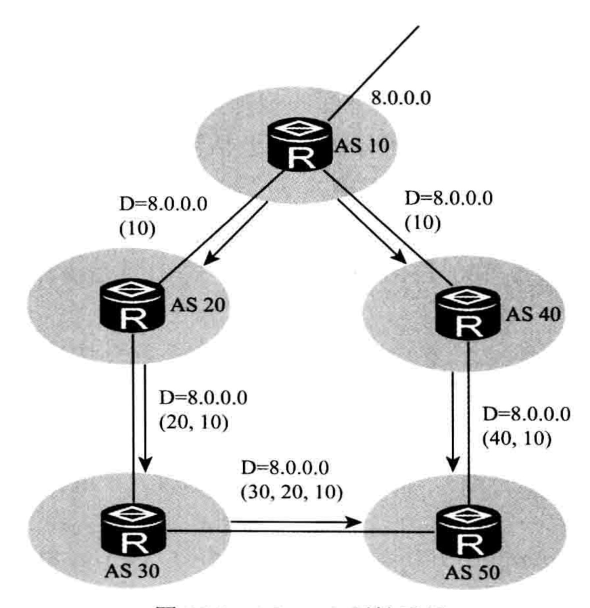


图 14-8 AS_Path 属性示例

缺省情况下，BGP 不会接受 AS_Path 中已包含本地 AS 号的路由，从而避免了形成路由环路的可能，与 RIP 的水平分割特性功能类似。也就是只有在 EBGP 对等体之间通

告路由时才会在 AS 路径列表中添加 AS 号，同一个 AS 中的通告不会添加 AS 号。如果某台 BGP 路由器从其外部对等体收到某条路由的 AS 路径列表中包含了自己的 AS 号，则该路由就知道出现了环路，因而将丢弃该路由。

同时，AS_Path 属性也可用于路由的选择和过滤。在其他因素相同的情况下，BGP 会优先选择路径较短的路由。如图 14-8 所示，AS 50 中的 BGP 路由器会优先选择经过 AS 40 的路径作为到目的地址 8.0.0.0 的最优路由。

在某些应用中，还可以使用路由策略来人为地增加 AS 路径的长度，以便更为灵活地控制 BGP 路由路径的选择。通过配置 AS 路径过滤列表，还可以针对 AS_Path 属性中所包含的 AS 号来对路由进行过滤。这里涉及到的就是路由策略，具体将在下章介绍。

14.3.4 NEXT_HOP 属性

Next_Hop（下一跳）属性也是公认必须遵守的 BGP 属性。因为 BGP 主要用于 AS 间网络的连接，所以它的“下一跳”仅是针对不同 AS 中 EBGP 对等体间的路由发布而言的，**是指下一个 AS，而不是指下一个路由器**，因为在 IBGP 对等体间的路由发布中其下一跳属性是不会改变的。

【经验之谈】动态路由（包括本书前面介绍的 RIP、OSPF、IS-IS 和本章所介绍的 BGP）的“下一跳”都是针对接收路由信息的设备而言的，而不是针对发送路由信息而言的，因为路由中的目的地址所在网络总是在通告路由的路由器之前，**即路由自身的路径与路由被通告的路径是相反的**。只有理解了这一点，才能理解下面介绍的“BGP 路由下一跳为路由器的出接口 IP 地址”的含义。另外，要注意的一点是，无论是 EBGP 对等体，还是 IBGP 对等体，不一定都是直接连接的，**非直接连接的 BGP 路由器之间也可建立 EBGP 或者 IBGP 对等体连接。**

通常情况下，Next_Hop 属性遵循下面的规则。

① BGP Speaker 在向 EBGP 对等体发布（包括转发）某条路由时，会把该路由信息的下一跳属性修改为**本地与对端建立 EBGP 对等体连接关系的出接口 IP 地址。**

如图 14-9 所示，AS 100 路由器产生到达 8.0.0.0 网络的路由并发布给 AS 200 路由器时，下一跳地址就是 AS 100 路由器与 AS 200 路由器连接时所用的出接口 IP 地址 1.1.1.1/24。

这里再次解释一下为什么该路由的下一跳会变成发送路由发布的 AS 100 中的路由器的出接口 IP 地址 1.1.1.1/24。因为对于接收这条路由的 AS200 中的路由器来说，它到达 1.1.1.1/24 的路由方向其实就是由 AS 100 中的路由器向它自己通告这条路由的反方向（也就是图中箭头方向的反方面），而在这个反方向中的下一跳正好就是 AS 100 中的路由器的出接口。

同理，AS 200 向 AS 300 中左边那台路由器转发从 AS 100 得到的路由发布时，其路由的下一跳地址为 AS 200 与 AS 300 中左边那台路由器相连时所用的出接口的 IP 地址 1.1.2.1/24。

② BGP Speaker 将**本地始发的路由**（也就是这条路由的目的网络就是直接连接在该 BGP Speaker 上）发布给 IBGP 对等体时，也会把该路由信息的下一跳属性设置为本地与

对端建立 IBGP 邻居关系的出接口 IP 地址。**但是收到该 IBGP 路由的 IBGP 对等体不会再转发给其他的 IBGP 对等体**，这是为了避免在 AS 内部出现路由环路。即 BGP Speaker 从 IBGP 对等体获得的 IBGP 路由不再向其他 IBGP 对等体发布。

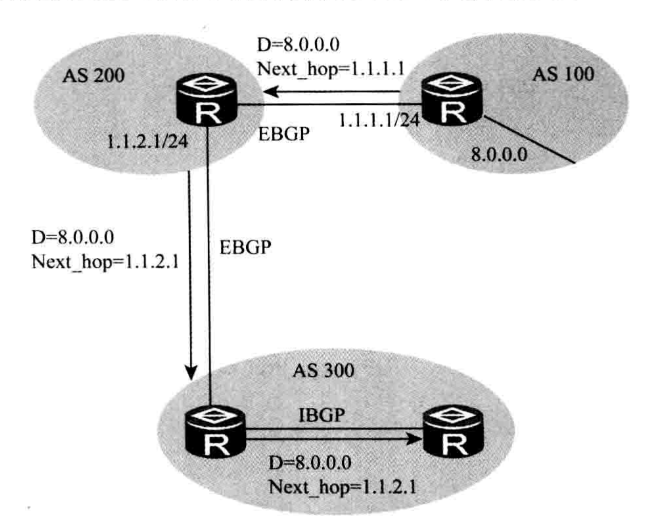


图 14-9　BGP 下一跳属性示例

③ BGP Speaker 在**向 IBGP 对等体转发从 EBGP 对等体学习到的路由时，不改变该路由信息的下一跳属性**（但通过配置也改为转发路由的 BGP 设备的出接口 IP 地址，具体会在本章后面介绍），**但收到转发的 EBGP 路由的 IBGP 对等体可以再转发给其他 IBGP 对等体。且如果配置了负载分担，路由被发给 IBGP 对等体时则会修改其下一跳属性。**

如图 14-9 所示，AS 300 左边那台路由器转发从 AS 200 获得的路由发布到相同区域中的右边那台路由器时，其下一跳没有改变，仍为 AS 200 与 AS 300 中左边那台路由器相连时所用的接口的 IP 地址 1.1.2.1/24。

14.3.5　LOCAL_PREF 属性

Local_Pref（本地优先级）属性是公认任意（也是所有 BGP 路由器都可识别，但可以不在 Update 报文中存在）的 BGP 属性，表明 BGP 路由器自身（**不是针对具体路由**）的 BGP 优先级（**Local_Pref 属性值越大，优先级越高**），用于判断流量**离开本地 AS 时**的最佳路由（**后面将要介绍的 MED 属性是进入 AS 时的最优路由**）。路由器配置了 Local_Pref 属性后，本路由器上所有的 BGP 路由都具有相同的本地优先级。

当一个 AS 内部的 BGP 的设备通过得到不同的 IBGP 对等体到达位于其他 AS 中的相同目的地址，但下一跳不同的多条路由时，将优先选择 Local_Pref 属性值较高的路由。**Local_Pref 属性仅在 IBGP 对等体之间交换和比较，不通告给其他 AS。**

如图 14-10 所示，在 Router D 上学习到了两条通过同一 AS 中的 IBGP 路由器路径到达 Router A 的路由，这时就可以使用本地优先级进行选路了，经过比较最终确定选择 Router C 作为从 AS 20 到 AS 10 的出口（如虚箭头方向），因为 Router C 中的 Local_Pref 属性值为 200，高于 Router B 中的 Local_Pref 属性值 100。

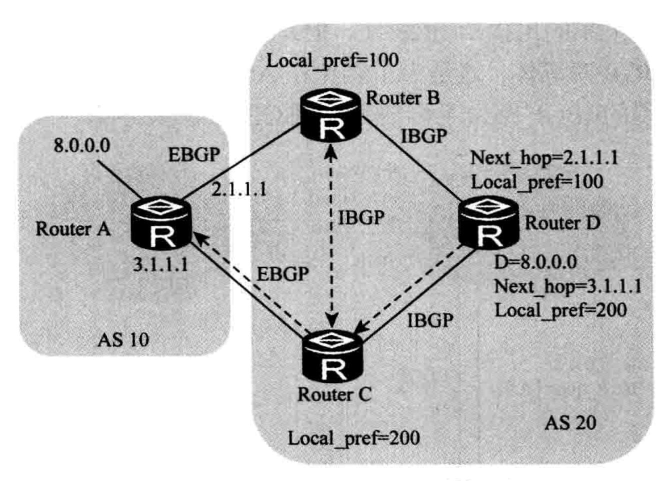


图 14-10 BGP Local_Pref 属性示例

14.3.6 MED 属性

MED（多出口）属性是一个可选非过渡（也就是不要求在 Update 必须存在，且不可向其他对等体通告）属性，**用于 EBGP 对等体判断流量进入其他 AS 时的最优路由。**

MED 属性仅在相邻两个 AS 之间交换，收到此属性的 AS 一方不会再将其通告给任何其他第三方 AS。当一个 BGP 路由器通过不同的 EBGP 对等体得到目的地址相同，但下一跳不同的多条路由时，在其他条件相同的情况下，**将优先选择 MED 值较小者作为进入 EBGP 对等体所在 AS 的最优路由，即 MED 值越小，优先级越高。**

如图 14-11 所示，从 AS 10 到 AS 20 的流量将选择 Router B 作为入口（如虚箭头方向），因为 Router B 中的 MED 值为 0，小于 Router C 中的 MED 值 100。

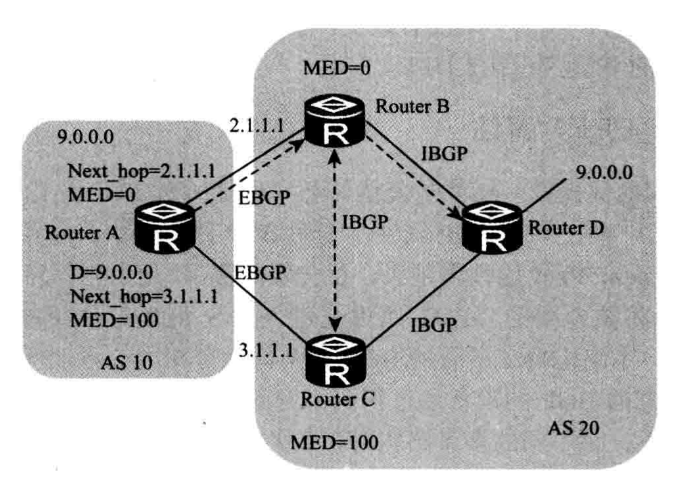


图 14-11 BGP MED 属性示例

一般情况下，EBGP 路由器只比较来自同一个其他 AS 中多个 EBGP 对等体路径的 MED 属性，不比较来自不同 AS 的 MED 值。若非要比较的话，则可以通过手动配置强制 BGP 比较来自不同 AS 的路由的 MED 属性值。如果路由没有配置 MED 属性，BGP

选路时将该路由的 MED 值按缺省值 0 来处理。

14.3.7　团体属性

Community（团体）属性是一个可选过渡（也是不要求在 Update 必须存在，但可向其他对等体通告）的 BGP 属性，是一组有相同特征的目的地址的 BGP 路由集合，用来简化路由策略的应用和降低维护管理的难度，因为这样可以为团体中的路由成员一次性配置相同的参数属性和路由策略，也可通过团体属性进行路由过滤。而且，团体中具体集合的路由数量没有物理上的边界，与其所在的 AS 无关，也就是可以是不同 AS 路径的路由。

BGP 团体属性可分为基本团体属性和扩展团体属性两种，下面分别予以介绍。

1. 基本团体属性

基本团体属性的“Type code”（类型代码）字段值是 8，属性取值占 32 位，可以解析为一个十进制数，也可以解析为 aa:nn 的格式，各占 16 位。32 位团体属性值中 0x00000000～0x0000FFFF 和 0xFFFF0000～0xFFFFFFFF 被保留。RFC1997 中规定，**前 16 位表示路由的源 AS 号，后 16 位可以理解为源 AS 划分的子 AS 号，也可用来标识路由来自不同的 IGP 路由类型，或者其他属性，如本地优先级值、MED 属性值等**，应用非常灵活。

RFC1997 还规定了以下几种公认的基本团体属性。

① INTERNET：缺省情况下，所有的路由都属于 INTERNET 团体。具有此属性的路由可以被通告给所有的 BGP 对等体。

② NO_EXPORT（属性值为十进制的 4 294 967 041，或者十六进制的 0xFFFFFF01）：具有此属性的路由在被收到后，不能被发布到本地 AS 之外。如果使用了联盟（Confederation），则不能被发布到 BGP 联盟之外，但可以发布给联盟中的其他子 AS。

说明　BGP 联盟其实就是一个 AS 下面的子 AS 划分，满足一些较大企业用户需要多个 AS，但又想进行集中路由域管理的需求。这样就在一个大的组织机构划分多个子网络管理区域，每个子区域独立分配成为 1 个子 AS，可以减少同一个 AS 中 BGP 路由的数量，提高了路由和管理效率。联盟子 AS 之间的 BGP 邻居是联盟 EBGP 关系，具体将在下节介绍。

③ NO_ADVERTISE（属性值为十进制的 4 294 967 042，或者十六进制的 0xFFFFFF02）：具有此属性的路由被接收后，不能被通告给任何其他的 BGP 对等体。

④ NO_EXPORT_SUBCONFED（属性值为十进制的 4 294 967 043，或者十六进制的 0xFFFFFF03）：具有此属性的路由被接收后，不能被通告到本地 AS 之外，也不能通告到联盟中的其他子 AS。

设备在收到带有这几个公认的团体属性的路由后，是自动按照 RFC1997 规定来执行的，不需要再配置路由策略。

2. 扩展团体属性

因为团体属性的使用越来越丰富，原有的 32 位定义已经不能满足各种应用，所以应运而生了扩展团体属性。扩展团体属性使用了新的“Type code”（为 16）和格式，在

RFC4360 中定义。比起原来的基本团体属性，扩展团体属性提供了更长的取值范围（占 64 位），以减少冲突的可能；同时，还增加了一个 Type 字段，可以使得路由策略直接基于扩展团体属性的 Type 字段进行操作。相当于将一些原来需要通过复杂的团体属性配置才能实现的功能，直接添加到了扩展团体属性的结构中。

扩展团体属性比较复杂，在此不作介绍。

14.4 路由反射器与联盟

在 BGP 中，为了防止路由环路的出现，对于 EBGP 路由和 IBGP 路由分别作了如下规定。

① 对于 AS 之间学习到的 EBGP 路由，通过 AS_Path 属性记录途经的 AS 路径，规定在收到带有本地 AS 号的路由将被直接丢弃。

② 对于 AS 内部学习到的 IBGP 路由，规定在收到路由后禁止向其他 IBGP 对等体发布。也就是 IBGP 对等体之间仅能学习到对等体（IBGP 的对等体可以不是直接连接的）之间的路由，不能学习到非邻居之间的路由。

从上面的说明可以看出，IBGP 设备之间只有对等体之间可以相互学习到路由，这样一来就带来了一个问题，即非 IBGP 对等体之间不能彼此交互路由信息，变成路由不可达了。为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。即假设在一个 AS 内部有 n 台设备，那么建立的 IBGP 连接数就为 $n(n-1)/2$。但这样一来，当一个 AS 中的 BGP 设备数目很多时，设备配置将十分复杂，而且配置后网络资源和 CPU 资源的消耗都很大。

为了解决以上问题，BGP 提供了两种解决方案，一个就是在 IBGP 对等体间使用路由反射器（Route Reflector，RR），另一个就是联盟（Confederation）。下面分别予以介绍。

14.4.1 路由反射器

在 RR 技术中，为一个 AS 内部的各 IBGP 设备定义了以下几种角色，如图 14-12 所示。

① 路由反射器（RR）：允许把从 IBGP 对等体学习到的路由反射到其他 IBGP 对等体，与 OSPF 网络中的 DR（指定路由器）或者 IS-IS 网络中的 DIS（指定 IS）类似。

② 客户机（Client）：与 RR 形成反射邻居关系的 IBGP 设备，类似于 OSPF 中的 DROther，或者 IS-IS 网络中的 DISOther。在 AS 内部，客户机只需要与 RR 直连，彼此交换路由信息，客户机之间无需直接连接，也无需交换路由信息。

③ 非客户机（Non-Client）：既不是 RR，也不是客户机的 IBGP 设备。在 AS 内部非客户机与 RR 之间，以及所有的非客户机之间仍然**必须建立全连接关系**。

④ 集群（Cluster）：路由反射器及其客户机的集合。通过专门的 Cluster_List 属性可防止集群间产生路由环路。

⑤ 始发者（Originator）：在 AS 内部始发 IBGP 路由的 BGP 设备。通过专门的 Originator_ID 属性可防止集群内产生路由环路。

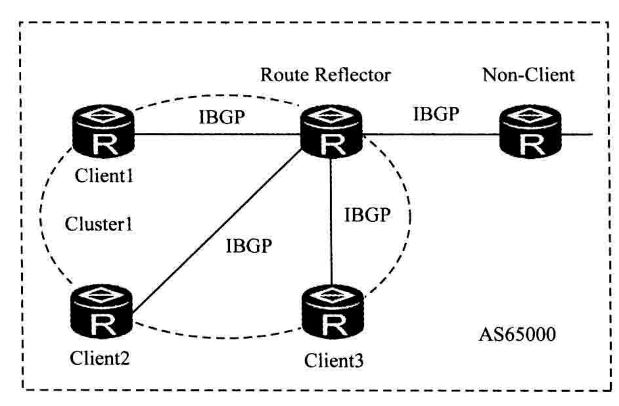


图 14-12　路由反射器中的相关角色

1. 路由反射器原理

在路由反射器技术中规定，同一集群内的客户机只需要与该集群的 RR 直接交换路由信息，因此客户机只需要与 RR 之间建立 IBGP 连接，不需要与其他客户机建立 IBGP 连接，从而减少了 IBGP 连接数量。如图 14-12 所示，在 AS65000 内，一台设备作为 RR，三台设备作为客户机，形成 Cluster1。此时，AS65000 中 IBGP 的连接数从配置 RR 前的 10 条减少到 4 条，不仅简化了设备的配置，也减轻了网络和 CPU 的负担。

RR 突破了“从 IBGP 对等体获得的 BGP 路由只能发布给它的 EBGP 对等体”的限制，并采用独有的 Cluster_List 属性和 Originator_ID 属性分别防止了集群之间和集群内部的路由环路出现。RR 向 IBGP 邻居发布路由规则如下。

① 从非客户机学习到的路由，发布给所有客户机。

② 从客户机学习到的路由，发布给所有非客户机和客户机（发起此路由的客户机除外）。

③ 从 EBGP 对等体学习到的路由，发布给所有的非客户机和客户机。

2. Cluster_List 属性

路由反射器和它的客户机组成一个集群（Cluster），使用 AS 内唯一的 Cluster ID 作为标识。为了防止集群间产生路由环路，路由反射器使用 Cluster_List 属性来记录路由经过的所有集群的 Cluster ID，类似于 EBGP 路由中所使用的 AS_PATH 属性。具体流程如下。

① 当一条路由第一次被 RR 通告的时候，RR 会把本地 Cluster ID 添加到 Cluster_List 的前面。如果没有 Cluster_List 属性，RR 就创建一个。

② 当 RR 接收到一条更新路由时，RR 会检查 Cluster_List。如果 Cluster_List 中已经有本地 Cluster ID，则丢弃该路由；否则，将其加入 Cluster List，然后通告该更新路由。

3. Originator_ID 属性

Originator_ID 由 RR 产生，使用路由始发者的 Router ID 进行标识，用于防止集群内产生路由环路。具体流程如下。

① 当一条路由第一次被 RR 通告的时候，RR 将路由始发者的 Originator_ID 属性加入这条路由，标识这条路由的发起设备。如果一条路由中已经存在了 Originator_ID 属性，则 RR 将不会创建新的 Originator_ID 属性。

② 当 IBGP 接收到这条路由的时候，将比较收到的 Originator_ID 和本地的 Router ID，如果两个 ID 相同，则丢弃该路由，否则，接收该更新路由。

4. 备份路由反射器

为增加网络的可靠性，防止单点故障对网络造成影响，有时需要在一个集群中配置一个以上的 RR。由于 RR 打破了从 IBGP 对等体收到的路由不能传递给其他 IBGP 对等体的限制，所以如果同一集群内存在多个 RR，则它们之间中又可能存在环路，因此这里又规定，同一集群中的所有 RR 必须使用相同的 Cluster ID，以避免 RR 之间的路由环路。

如图 14-13 所示，路由反射器 RR1 和 RR2 在同一个集群内，配置了相同的 Cluster ID。下面是备份路由反射器解决路由环路的具体流程。

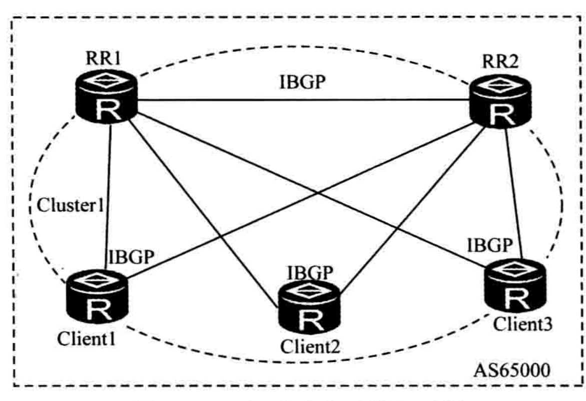


图 14-13 备份路由反射器示例

① 当客户机 Client1 从 EBGP 对等体接收到一条更新路由时，它将通过 IBGP 同时向 RR1 和 RR2 通告这条路由。

② RR1 和 RR2 在接收到该更新路由后，将本地 Cluster ID 添加到 Cluster List 前面，然后向其他的客户机（Client2、Client3）通告。

③ 当 Client2、Client3 客户向 RR1 和 RR2 进行路由发布时，RR1 和 RR2 有可能收到原来由自己向客户机通告的路由。这时 RR1 和 RR2 会检查路由发布中的 Cluster List，如果发现自己的 Cluster ID 已经包含在通告路由的 Cluster List 中，就丢弃该更新路由，从而避免了路由环路。

5. 多集群路由反射器

一个 AS 中可以存在多个集群，各个集群的 RR 之间可以建立 IBGP 对等体。当 RR 所处的网络层不同时，可以将较低网络层次的 RR 配成客户机，形成分级 RR。当 RR 所处的网络层相同时，可以将不同集群的 RR 全连接，形成同级 RR。在实际的 RR 部署中，常用的是分级 RR 的场景。

如图 14-14 所示，ISP 为 AS100 提供 Internet 路由。AS100 内部分为两个集群，其中 Cluster1 内的 4 台设备是核心路由器，采用备份 RR 的形式保证可靠性；而 Cluster2 内的两台设备是下级路由器，采用单 RR 结构。

如图 14-15 所示，一个骨干网被分成多个集群。各集群的 RR 间互为非客户机关系，并建立全连接。此时，虽然每个客户机只与所在集群的 RR 建立 IBGP 连接，但所有 RR

和客户机都能收到全部路由信息。

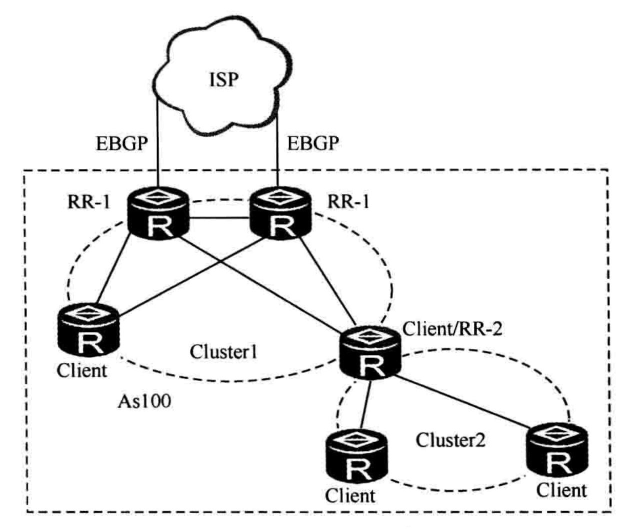


图 14-14　分级路由反射器示例

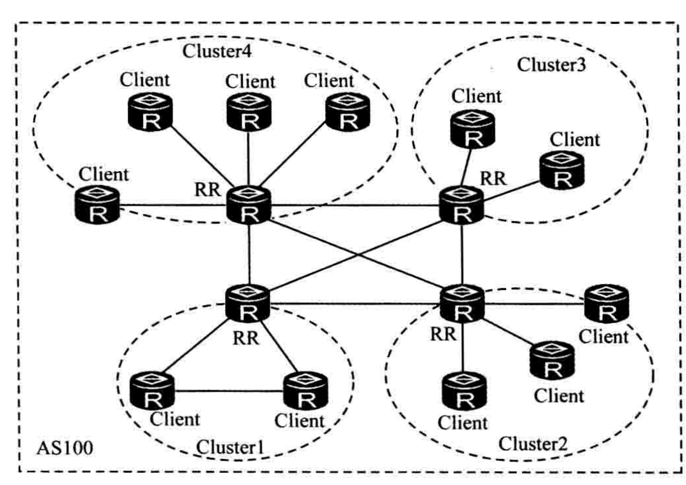


图 14-15　同级路由反射器示例

14.4.2　BGP 联盟

解决 AS 内部的 IBGP 网络连接激增问题，除了可使用上节介绍的路由反射器解决方案之外，还可以使用联盟（Confederation）技术。

联盟将一个 AS 划分为若干个子 AS。每个子 AS 内部建立 IBGP 全连接关系，子 AS 之间建立联盟 EBGP 连接关系，但联盟外部 AS 仍会认为联盟是一个 AS。配置联盟后，**原 AS 号将作为每个路由器的联盟 ID**。这样有两个好处：一是可以保留原有的 IBGP 属性，包括 Local Preference 属性、MED 属性和 Next_Hop 属性等；二是联盟相关的属性在传出联盟时会自动被删除，即管理员无需在联盟的出口处配置过滤子 AS 号等信息的操作。

如图 14-16 所示，AS100 使用联盟后被划分为 3 个子 AS：AS65001、AS65002 和 AS65003，使用 AS100 作为联盟 ID。此时 IBGP 的连接数量从 10 条减少到 4 条，不仅简化了设备的配置，也减轻了网络和 CPU 的负担。而 AS100 外的 BGP 设备因为仅知道 AS100 的存在，并不知道 AS100 内部的联盟关系，所以不会增加 CPU 的负担。

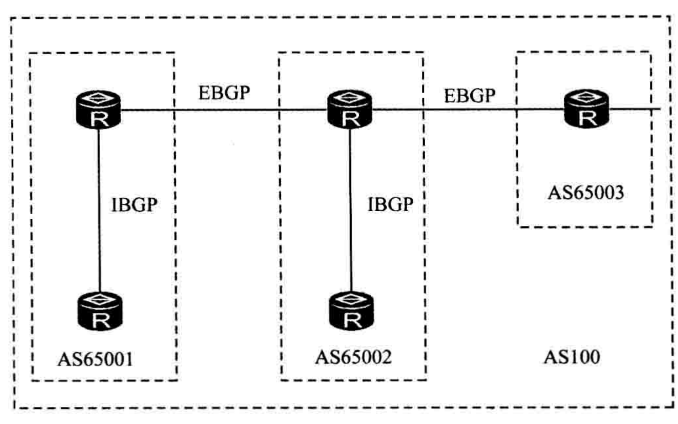


图 14-16　BGP 联盟示例

联盟的缺陷是：从非联盟方案向联盟方案转变时，要求路由器重新进行配置，逻辑拓扑也要改变。在大型 BGP 网络中，路由反射器和联盟可以被同时使用。表 14-5 从配置、设备连接和应用方面对比了路由反射器和联盟。

表 14-5　路由反射器与联盟的比较

路由反射器	联盟
不需要更改现有的网络拓扑，兼容性好	需要改变逻辑拓扑
配置方便，只需要对作为反射器的设备进行配置，客户机并不需要知道自己是客户机	所有设备需要重新进行配置
集群与集群之间仍然需要全连接	联盟的子 AS 之间是特殊的 EBGP 连接，不需要全连接
适用于中、大规模网络	适用于大规模网络

14.5　BGP 工作原理

通过前面的学习，我们已经知道，BGP 路由有许多属性，而这些属性又影响着最终的路由选择。另外，BGP 本身不产生、发现路由，它是将各种 IGP 路由、静态路由、直连路由引入后向其他 AS 或者本地 AS 的对等体进行发布。本节就要介绍这几个方面的工作原理，即 BGP 的路由选路规则、BGP 对等体交互原理以及 BGP 路由与 IGP 路由的交互原理。

14.5.1　BGP 协议的选路规则

由于 BGP 连接的是一个非常复杂，且可能混合多种 IGP 路由协议的网络，因此就

可能通过不同接口学习到多条到达同一目的地的不同路径、不同协议的路由，这就决定了 BGP 在路由选择方面要考虑到许多方面。

为了指导路由选路，BGP 规定了下一跳策略（即“首先丢弃下一跳（Next_Hop）不可达的路由”的策略）和路由选路规则，其中下一跳策略的优先级比 BGP 路由选路规则高。在执行完下一跳策略后，BGP 使用如下选路规则进行路由选择（由上至下优先级依次降低）。

① 优选协议首选值（Preferred-value）属性值最高的路由。协议首选值（PrefVal）是华为设备的特有属性，该属性仅在本地有效。

② 优选本地优先级（Local_Pref）属性值最高的路由。如果路由没有本地优先级，BGP 选路时将该路由按缺省的本地优先级 100 来处理。通过执行 **default local-preference** 命令可以修改 BGP 路由的缺省本地优先级。

③ 依次优选手动聚合路由、自动聚合路由、**network** 命令引入的路由、**import-route** 命令引入的路由、从对等体学习的路由。

④ 优选 AS 路径（AS_Path）最短的路由。

⑤ 依次优选 Origin 类型为 IGP、EGP、Incomplete 的路由。

⑥ 对于来自同一 AS 的路由，优选 MED 属性值最低的路由。

⑦ 依次优选 EBGP 路由、IBGP 路由。

⑧ 优选到 BGP 下一跳 IGP 度量值（metric）最小的路由。但在 IGP 类型路由协议中，对到达同一目的地址的不同路由，不同 IGP 路由协议会根据本身的路由算法计算路由的度量值。

⑨ 优选 Cluster_List 最短的路由。

⑩ 优选 Router ID 最小的设备发布的路由。但如果该路由携带 Originator_ID 属性，选路过程中将比较 Originator_ID 的大小，不比较 Router ID，优选 Originator_ID 最小的路由。

⑪ 优选从具有最小 IP Address 的对等体学来的路由。

说明　当到达同一目的地址存在多条等价路由时，可以通过 BGP 等价负载分担实现均衡流量的目的。形成 BGP 等价负载分担的条件是以上“BGP 选择路由的策略”中的 1～8 条规则中需要比较的属性值完全相同。

14.5.2　BGP 对等体交互原理

BGP 对等体的建立、更新和删除等交互过程主要有 5 种报文、6 种状态机和 5 个原则。

1. 5 种 BGP 的报文

BGP 对等体间通过以下 5 种报文进行信息交互，其中 Keepalive 报文为周期性发送，其余报文为触发式发送（它们的报文格式参见 14.2 节）。

① Open 报文：用于建立 BGP 对等体连接。

② Update 报文：用于在对等体之间交换路由信息。

③ Notification 报文：用于中断 BGP 连接。

④ Keepalive 报文：用于保持 BGP 连接。

⑤ Route-refresh 报文：用于在改变路由策略后请求对等体重新发送路由信息。只有支持路由刷新（Route-refresh）能力的 BGP 设备会发送和响应此报文。

2. 6 种 BGP 状态机

在 BGP 对等体的交互过程中存在 6 种状态机：空闲（Idle）、连接（Connect）、活跃（Active）、Open 报文已发送（OpenSent）、Open 报文已确认（OpenConfirm）和连接已建立（Established）。这 6 种状态机的转换过程如图 14-17 所示。其中，在 BGP 对等体建立的过程中，使用了 Idle、Active 和 Established 三种状态机。

① Idle 状态是 BGP 初始状态。在 Idle 状态下，BGP 拒绝邻居发送的连接请求。只有在收到本设备的 Start（开始）事件后，BGP 才开始尝试和其他 BGP 对等体进行 TCP 连接，并转换至 Connect（连接）状态。

说明 Start 事件是由一个操作者配置一个 BGP 过程，或者重置一个已经存在的过程，或者路由器软件重置 BGP 过程引发的。任何状态中收到 Notification 报文或 TCP 拆链通知等 Error（错误）事件后，BGP 都会转换至 Idle 状态。

② 在 Connect 状态下，BGP 启动连接重传定时器（Connect Retry），等待 TCP 完成连接。

• 如果 TCP 连接成功，那么本地 BGP 向 BGP 对等体发送 Open 报文，并转换至 OpenSent 状态。

• 如果 TCP 连接失败，那么本地 BGP 转换至 Active 状态。

• 如果连接重传定时器超时后本地 BGP 仍没有收到 BGP 对等体的响应，那么本地 BGP 会继续尝试和其他 BGP 对等体进行 TCP 连接，停留在 Connect 状态。

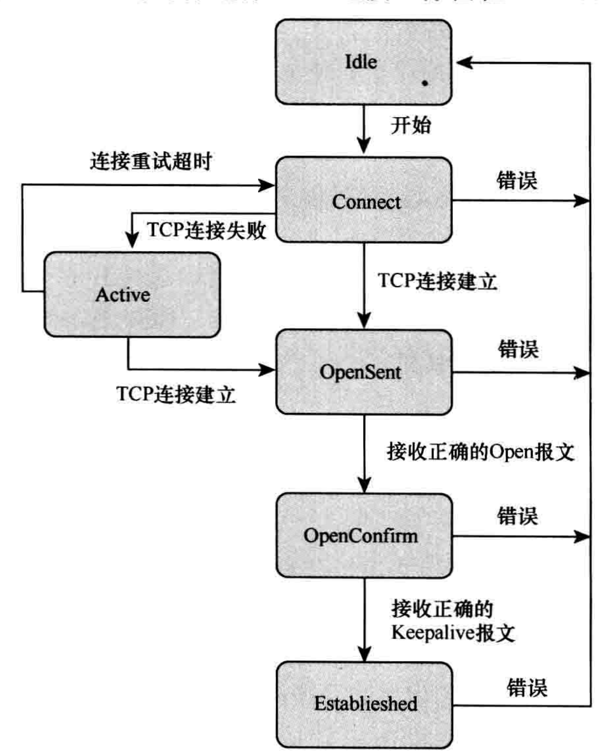


图 14-17　BGP 对等体交互中的状态机转换流程

③ 在 Active 状态下，本地 BGP 总是在试图建立 TCP 连接。

- 如果 TCP 连接成功，那么本地 BGP 向 BGP 对等体发送 Open 报文，关闭连接重传定时器，并转换至 OpenSent 状态。
- 如果 TCP 连接失败，那么本地 BGP 停留在 Active 状态。
- 如果连接重传定时器超时后本地 BGP 仍没有收到 BGP 对等体的响应，那么本地 BGP 转换至 Connect 状态。

④ 在 OpenSent 状态下，本地 BGP 等待对等体的 Open 报文，并对收到的 Open 报文中的 AS 号、版本号、认证码等进行检查。

- 如果收到的 Open 报文正确，那么本地 BGP 向 BGP 对等体发送 Keepalive 报文，并转换至 OpenConfirm 状态。
- 如果发现收到的 Open 报文有错误，那么本地 BGP 向 BGP 对等体发送 Notification 报文给对等体，并转换至 Idle 状态。

⑤ 在 OpenConfirm 状态下，本地 BGP 等待来自 BGP 对等体的 Keepalive 或 Notification 报文。如果收到 Keepalive 报文，则转换至 Established 状态；如果收到 Notification 报文，则转换至 Idle 状态。

⑥ 在 Established 状态下，本地 BGP 可以和 BGP 对等体交换 Update、Keepalive、Route-refresh 报文和 Notification 报文。

- 如果收到正确的 Update 或 Keepalive 报文，那么本地 BGP 就认为对端处于正常运行状态，将保持 BGP 连接。
- 如果收到错误的 Update 或 Keepalive 报文，那么本地 BGP 发送 Notification 报文通知对端，并转换至 Idle 状态。
- Route-refresh 报文不会改变 BGP 状态。
- 如果收到 Notification 报文，那么本地 BGP 转换至 Idle 状态。
- 如果收到 TCP 拆链通知，那么本地 BGP 断开连接，转换至 Idle 状态。

3. BGP 对等体之间的 5 种交互原则

BGP 设备将最优路由加入 BGP 路由表，形成 BGP 路由。BGP 设备与 BGP 对等体间成功建立邻居关系后，缺省情况下将采取以下 5 种交互原则。

- **从 IBGP 对等体获得的 BGP 路由，只发给它的 EBGP 对等体。**
- **从 EBGP 对等体获得的 BGP 路由，发给它所有 EBGP 和 IBGP 对等体。**
- 当存在多条到达同一目的地址的有效路由时，BGP 设备只将最优路由发布给对等体。
- 路由更新时，BGP 设备**只发送要更新的 BGP 路由，不是发送整个路由表。**
- 所有对等体发送的路由，BGP 设备都会接收。

14.5.3 BGP 与 IGP 交互原理

由于 BGP 与 IGP 在设备中使用不同的路由表，因此为了实现不同 AS 间相互通信，BGP 需要与 IGP 进行交互，即 BGP 路由表和 IGP 路由表相互引入。

1. BGP 引入 IGP 路由

BGP 协议本身不产生、发现路由，因此需要将其他路由引入 BGP 路由表，实现 AS

间的路由互通。当一个 AS 需要将路由发布给其他 AS 时，AS 边缘路由器会在 BGP 路由表中引入 IGP 的路由。为了更好地规划网络，BGP 在引入 IGP 的路由时，可以使用路由策略进行路由过滤和路由属性设置，也可以设置 MED 属性指导 EBGP 对等体判断流量进入 AS 时选路。

BGP 引入路由时支持 Import 和 Network 两种方式。

① Import 方式是按协议类型，将 RIP、OSPF、ISIS 等协议的路由引入到 BGP 路由表中。为了保证引入的 IGP 路由的有效性，Import 方式还可以引入静态路由和直连路由。

② Network 方式是逐条**将 IP 路由表中已经存在的路由**引入到 BGP 路由表中，比 Import 方式更精确。

2. IGP 引入 BGP 路由

当一个 AS 需要引入其他 AS 的路由时，AS 边缘路由器会在 IGP 路由表中引入 BGP 的路由。为了避免大量 BGP 路由对 AS 内设备造成影响，当 IGP 引入 BGP 路由时，可以使用路由策略进行路由过滤和路由属性设置。

如图 14-18 所示，某公司海外市场部所在区域 AS100 部署 OSPF 网络，国内研发部所在区域 AS200 部署 IS-IS 网络，现要求 AS100 与 AS200 通过部署 BGP 实现互通。

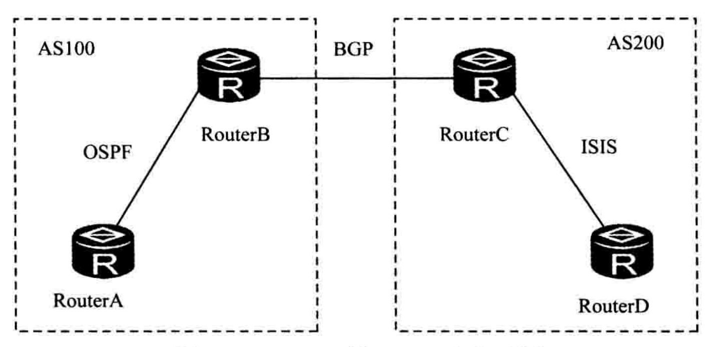


图 14-18　IGP 引入 BGP 路由示例

这就同时涉及到了 BGP 引入 IGP 路由，IGP 引入 BGP 路由。为了实现以上要求，必须让 AS100 中的设备知道 AS200 的路由，同时 AS200 中的设备知道 AS100 的路由。配置方法是在 RouterC 上部署 BGP 引入本地 AS 中的 IGP IS-IS 路由，使 RouterC 的 BGP 路由表中存在 AS200 中的路由，并通过 EBGP 把引入的路由发布给 RouterB，然后在 RouterB 上部署 OSPF 引入 BGP 路由，实现 AS100 内设备知道 AS200 的路由；同理，要在 RouterB 上部署 BGP 引入本地 AS 中的 IGP OSPF 路由，使 RouterB 的 BGP 路由表中存在 AS100 中的路由，并通过 EBGP 把引入的路由发布给 RouterC，然后在 RouterC 上部署 IS-IS 引入 BGP 路由，实现 AS200 内设备知道 AS100 的路由，最终实现两个 AS 中的设备能够互通。

14.6　BGP 的基本功能配置与管理

与本书前面介绍的 RIP、OSPF、IS-IS 协议一样，虽然 BGP 协议本身功能很强大，配置也很复杂，但是要建立一个基本的 BGP 网络，配置还是比较简单的，仅需要配置

BGP 的一些基本功能。同时，BGP 基本功能的配置也是组建 BGP 网络的基础，是能够使用 BGP 其他功能的前提。但在配置 BGP 的基本功能之前，也需要先配置接口的 IP 地址，使相邻节点的网络层可达。

因为 BGP 中可以把一些需要配置相同属性的对等体配置为一个对等体组（**一般是仅在比较大，存在较多 BGP 设备的网络中使用对等体组进行配置**），同时又有 EBGP 对等体组和 IBGP 对等体组之分，所以在 BGP 基本功能的配置上，要有所区分。总体来说，BGP 基本功能所包括的配置任务如表 14-6 所示（要注意配置顺序），要根据不同的配置对象选择所需的配置任务（Y 表示要配置，N 表示不需要配置）。

表 14-6　BGP 基本功能的配置流程

配置任务	配置单个对等体	配置 IBGP 对等体组	配置 EBGP 对等体组
（1）启动 BGP 进程	Y	Y	Y
（2）配置 BGP 对等体	Y	N	Y
（3）配置 BGP 对等体组	N	Y	Y
（4）配置 BGP 引入路由	Y	Y	Y

14.6.1　启动 BGP 进程

BGP 是一种用于域间的动态路由协议。当 BGP 设备各接口连接的都是位于同一 AS 中的设备时，其运行的是 IBGP，当设备至少有一个接口连接的是其他 AS 中的设备时，其运行的是 EBGP。**但每台 BGP 设备只能运行于一个 AS 内**，即只能指定一个本地 AS 号。同时，**BGP 是单进程路由协议，所以它本身没有进程号，只是用所处的 AS 号来进行标识。**

BGP 进程的配置其实就是为设备指定所处 AS，配置用于在 BGP 网络中唯一标识设备的路由器 ID 的过程，具体配置步骤如表 14-7 所示。

表 14-7　启动 BGP 进程的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明如下 ● *as-number-plain*：二选一参数，指定整数形式的 AS 号，取值范围为 1～4 294 967 295 的整数 ● *as-number-dot*：二选一参数，指定点分形式的 AS 号，格式为 *x.y*，*x* 和 *y* 都是整数形式，*x* 的取值范围为 1～65 535 的整数，*y* 的取值范围为 0～65 535 的整数 缺省情况下，BGP 是关闭的，可用 **undo bgp** [*as-number-plain* | *as-number-dot*]命令关闭指定进程的 BGP。但一个 BGP 设备只能位于一个 AS 中，即只能为 BGP 设备配置一个 AS 号
3	**router-id** *ipv4-address* 例如：[Huawei-bgp] **router-id** 1.1.1.1	配置 BGP 设备的 Router ID。参数 *ipv4-address* 用来指定设备的 Router ID，为类似于 IP 地址的点分十进制格式。为了提高网络的稳定性，通常建议将 Router ID 手动配置为 Loopback 接口地址，因为 Loopback 接口一旦创建，永远有效 【注意】改变 Router ID 或删除已配置的 Router ID 时，BGP 会话将重置 缺省情况下，BGP 选择 Router ID 依次优选**在系统视图下**通过 **router id** *router-id* 命令配置的 Router ID、Loopback 接口最大的 IP 地址、接口最大 IP 地址、IP 地址“0.0.0.0”

14.6.2 配置 BGP 对等体

BGP 中的“对等体”就是类似于 RIP、OSPF 和 IS-IS 中的邻居，但 BGP 的对等体不一定就是直连的设备，所以在 BGP 中需要手动指定对等体，**且需要在对等体双方分别配置**。

配置 BGP 对等体时，如果指定的对等体所属的 AS 编号与本地 AS 编号相同，表示配置 IBGP 对等体；如果指定对等体所属的 AS 编号与本地 AS 编号不同，表示配置 EBGP 对等体。为了增强 BGP 连接的稳定性，推荐使用路由可达的 Loopback 接口地址建立 BGP 连接。

BGP 对等体可以一个个单独配置，但如果有大量对等体的属性配置相同，则可以采用 BGP 对等体组配置方式。本节仅介绍单独配置方式，具体配置步骤如表 14-8 所示（**需要在对等体双方分别配置**），对等体组配置方式将在下节介绍。

表 14-8　　配置 BGP 对等体的步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见上节表 14-7 中的第 2 步
3	**peer** *ipv4-address* **as-number** { *as-number-plain* | *as-number-dot* } 例如：[Huawei-bgp] **peer** 1.1.1.2 **as-number** 100	创建 BGP 对等体。命令中的参数说明如下 ● *ipv4-address*：指定要创建 BGP 对等体连接的对等体的 IP 地址 ● *as-number-plain*：二选一参数，指定对等体所属 AS 的整数形式，取值范围为 1～4 294 967 295 的整数 ● *as-number-dot*：二选一参数，指定对等体所属 AS 的点分形式，格式为 *x.y*，*x* 和 *y* 都是整数形式，*x* 的取值范围为 1～65 535 的整数，*y* 的取值范围为 0～65 535 的整数 缺省情况下，没有创建 BGP 对等体，可用 **undo peer** *ipv4-address* 命令删除指定的对等体
4	**peer** *ipv4-address* **connect-interface** *interface-type interface-number* [*ipv4-source-address*] 例如：[Huawei-bgp] **peer** 1.1.1.2 **connect-interface** gigabitethernet 1/0/0	（可选）指定 BGP 对等体之间建立 TCP 连接会话的源接口和源地址。命令中的参数说明如下 ● *ipv4-address*：指定要配置建立 TCP 连接会活的源接口和源 IP 地址的对等体的 IP 地址 ● *interface-type interface-number*：指定本地设备与由参数 *ipv4-address* 指定的对等体建立 TCP 连接会话的源接口，可以是物理接口，也可以是像 Loopback 这样的是逻辑接口。**当使用 Loopback 接口建立 BGP 连接时，建议对等体两端同时配置本命令**，以保证两端 TCP 连接的接口和地址的正确性。如果仅有一端配置该命令，可能导致 BGP 连接建立失败 ● *ipv4-source-address*：可选参数，指定本地设备与由参数 *ipv4-address* 指定的对等体建立 TCP 连接会话的源 IP 地址。**仅当源接口配置了多个 IP 地址时才需要指定本参数** 缺省情况下，BGP 使用与邻居直连的物理接口作为 TCP 连接的源接口和源 IP 地址，可用 **undo peer** *ipv4-address* **connect-interface** 命令恢复缺省设置

（续表）

步骤	命令	说明
5	**peer** *ipv4-address* **ebgp-max-hop** [*hop-count*] 例如：[Huawei-bgp] **peer** 1.1.1.2 **as-number** 200	（可选）指定建立 **EBGP** 连接（**不能是 IBGP 连接**）允许的最大跳数，**以允许 BGP 与非直连网络上的设备建立 EBGP 对等体连接**。命令中的参数说明如下 ● *ipv4-address*：指定要配置建立 EBGP 对等体连接所允许的最大跳数的对等体的 IP 地址 ● *hop-count*：可选参数，指定允许的最大跳数，范围为 1～255 的整数，缺省值为 255。当最大跳数指定为 1 时，表示建立的是直连 EBGP 连接，**则不能与非直连网络上的设备建立 EBGP 对等体连接。当 BGP 使用 Loopback 口建立 EBGP 对等体时，必须指定本参数≥2，否则邻居无法建立** 【注意】如果在 EBGP 连接的其中一端配置了本命令，另一端也需要配置本命令 **缺省情况下，只能在物理直连链路上建立 EBGP 连接**，可用 **undo peer** *ipv4-address* **ebgp-max-hop** 命令恢复缺省配置
6	**peer** *ipv4-address* **description** *description-text* 例如：[Huawei-bgp] **peer** 1.1.1.2 **description** ISP1	（可选）配置对等体的描述信息。命令中的参数说明如下 ● *ipv4-address*：指定要配置对等体描述信息的对等体的 IP 地址 ● *description-text*：指定对等体描述信息，1～80 个字符，可以是字母和数字，支持空格 缺省情况下，没有配置对等体的描述信息，可用 **undo peer** *ipv4-address* **description** 命令删除指定对等体的描述信息
7	**ipv4-family multicast** 例如：[Huawei-bgp]**ipv4-family multicast**	（可选）使能 BGP 的 IPv4 组播地址族，并进入 BGP 的 IPv4 组播地址族视图。**仅当在 IPv4 组播网络中配置 BGP 对等体才需要配置本步骤** 缺省情况下，进入 BGP-IPv4 单播地址族视图，可用 **undo ipv4-family multicast** 命令删除 BGP 的 IPv4 组播地址族视图下的所有配置
8	**peer** *ipv4-address* **enable** 例如：[Huawei-bgp-af-multicast] **peer** 1.1.1.2 **enable**	（可选）为 BGP 对等体使能 MP-BGP 功能，使之成为 MP-BGP 对等体（**具体使能的是哪种对等体，要视本命令是在哪个地址族视图下配置的**）。命令中的 *ipv4- address* 参数用来指定对等体的 IP 地址。**仅当需要在非 BGP-IPv4 单播地址族下建立 BGP 对等体时才需要配置本步骤，因为 BGP-IPv4 单播地址族下的对等体功能是缺省使能的** 【说明】本命令不仅可以在 IPv4 组播地址族下使用，还可以在 BGP 视图、BGP-IPv4 单播地址族、BGP-VPNv4 地址族下使用，用于使能对应地址族下与指定对等体之间交换相关路由信息的功能。当 **undo default ipv4-unicast** 命令去使能在 BGP-IPv4 单播地址族下的 BGP 对等体功能后，创建的 BGP 对等体需要在 BGP 视图下或者 BGP-IPv4 单播地址族视图下使用本命令使能 IPv4 单播地址族下 BGP 对等体功能 缺省情况下，只有 BGP-IPv4 单播地址族的对等体是自动使能的，可用 **undo peer** *ipv4-address* **enable** 命令去使能指定对等体的 MP-BGP 功能

14.6.3 配置 BGP 对等体组

在大型 BGP 网路中，对等体的数目众多，配置和维护极为不便。这时，对于那些存在相同配置的 BGP 对等体可以通过一次性配置将它们加入一个 BGP 对等体组进行批量配置，以简化管理的难度，并提高路由发布效率。**但对等体组中的成员可以配置不同的路由接收策略，也可以配置不同的路由发布策略。**

同样，这里所说的“对等体组”也可以是 IBGP 对等体组，或者 EBGP 对等体组，具体的配置步骤如表 14-9 所示。对比上节介绍的 BGP 对等体配置可以看出，它们的配置方法非常类似，只不过这里是针对对等体组进行的配置，将在对等组中所有成员上生效。

说明 当对单个对等体和其所加入的对等体组同时配置了某个功能时，对单个对等体的配置优先生效。重复表中的步骤 5，可向对等体组中加入多个对等体。当需要将 EBGP 对等体加入同一对等体组时，**必须先按上节介绍的方法配置各个 EBGP 对等体，**然后配置步骤 5；但当只需要将 IBGP 对等体加入同一对等体组时，则可以直接配置步骤 5，系统会自动在 BGP 视图下创建该对等体，并设置其 AS 编号为对等体组的 AS 号。

当使用 Loopback 接口或子接口的 IP 地址建立 BGP 对等体连接时，建议对等体两端同时配置表中的步骤 6，以保证两端连接的正确性。如果仅有一端配置该命令，可能导致 BGP 连接建立失败。当使用 Loopback 接口建立 EBGP 对等体连接时，必须配置步骤 7，且 ***hop-count*** 参数值必须 **≥2**，否则 **EBGP** 对等体连接将无法建立。

表 14-9　　BGP 对等体组的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**group** *group-name* [**external** | **internal**] 例如：[Huawei-bgp] **group ex internal**	创建对等体组。命令中的参数和选项说明如下 ● *group-name*：指定所创建的对等体组的名称，1～47 个字符，区分大小写，不支持空格 ● **external**：二选一可选项，指定创建 EBGP 对等体组 ● **internal**：二选一可选项，指定创建 IBGP 对等体组。当不指定对等体组是 IBGP 对等体组还是 EBGP 对等体组时，**缺省为创建 IBGP 对等体组** 【说明】如果 BGP 对等体组内的对等体在某属性配置上与其所加入的对等体组上的相同属性配置不一致，则当在恢复该对等体上对应属性配置时，该对等体会从对其所加入的对等体组上继承对应属性配置 缺省情况下，系统中未创建对等体组，可用 **undo group** *roup-name* 命令删除指定的对等体组。但删除对等体组会导致该组内没有配置 AS 号的对等体间中断连接，建议先删除掉对等体组里没有配置 AS 号的对等体或给这些对等体先配置上 AS 号，然后删除对等体组，这样就不会中断对等体中的连接

（续表）

步骤	命令	说明
4	**peer** *group-name* **as-number** { *as-number-plain* | *as-number-dot* } 例如：[Huawei-bgp] **peer** ex **as-number** 100	（可选）配置 EBGP 对等体组的 AS 号，**如果是 IBGP 对等体组则不用配置本步骤**。命令中的参数 *group-name* 用来指定要配置 AS 号的对等体组名称，其他参数说明参见 14.6.2 小节表 14-8 中的第 3 步说明。**要求所有对等体组成员都处于同一个 AS 中** 缺省情况下，没有指定 EBGP 对等体组 AS 号，可用 **undo** *group-name* **peer as-number** 命令删除为指定的对等体组配置 AS 号
5	**peer** *ipv4-address* **group** *group-name* 例如：[Huawei-bgp] **peer** 1.1.1.2 **group** ex	向对等体组中加入对等体，但如果是向 EBGP 对等体组中加入 EBGP 对等体，则需先按 14.2.6 小节介绍的方法配置好各个 EBGP 对等体，再来配置本步骤；如果是向 IBGP 对等体组中加入 IBGP 对等体，可直接进行本步骤。命令中的参数 *ipv4-address* 和 *group-name* 分别用来指定要加入对等体组的对等体 IP 地址以及所加入的对等体组的名称 **需要对本地对等体组中的每个对等体成员执行本步操作** 缺省情况下，对等体组中没有对等体，可用 **undo peer** *pv4-ddress* **group** *group-name* 命令从指定的对等体组中移除指定的对等体
6	**peer** *group-name* **connect-interface** *interface-type interface-number* [*ipv4-source-address*] 例如：[Huawei-bgp] **peer** ex **connect-interface** gigabitethernet 1/0/0	（可选）指定本地设备与 BGP 对等体组中的对等体成员之间建立 TCP 连接会话的源接口和源 IP 地址。命令中的参数 *group-name* 用来指定要配置建立 TCP 连接会话的源接口和源地址的 BGP 对等体所属的对等体组的名称，其他参数说明参见 14.6.2 小节表 14-8 中的第 4 步说明 **配置本命令后，本地设备与所有对等体组成员之间的 TCP 连接会话使用相同的源接口和源 IP 地址** 缺省情况下，BGP 使用与邻居直连的物理接口作为 TCP 连接的源接口，可用 **undo peer** *group-name* **connect-interface** 命令恢复缺省设置
7	**peer** *group-name* **ebgp-max-hop** [*hop-count*] 例如：[Huawei-bgp] **peer** ex **as-number** 200 ebgp-maxhop2	（可选）指定本地设备与对等体组中的对等体成员建立 **EBGP** 连接（**不能是 IBGP 连接**）时所允许的最大跳数，以允许 BGP 与非直连网络上的设备建立 EBGP 对等体连接。命令中的参数 *group-name* 用来指定要配置 EBGP 对等体连接允许的最大跳数的 EBGP 对等体组名称，其他参数说明参见 14.6.2 小节表 14-8 中第 5 步的说明 缺省情况下，只能在物理直连链路上建立 EBGP 连接，可用 **undo peer** *group-name* **ebgp-max-hop** 命令恢复缺省配置
8	**peer** *group-name* **description** *description-text* 例如：[Huawei-bgp] **peer** ex **description** ISP1	（可选）配置对等体组的描述信息。命令中的参数 *group-name* 用来指定要配置描述信息的对等体组名称，其他参数说明参见 14.6.2 小节表 14-8 中第 6 步的说明 缺省情况下，没有配置对等体组的描述信息，可用 **undo peer** *group-name* **description** 命令删除指定对等体组的描述信息
9	**ipv4-family multicast** 例如：[Huawei-bgp]**ipv4-family multicast**	（可选）使能 BGP 的 IPv4 组播地址族，并进入 BGP 的 IPv4 组播地址族视图。**仅当在 IPv4 组播网络中配置 BGP 对等体组才需要配置本步骤** 缺省情况下，进入 BGP-IPv4 单播地址族视图，可用 **undo ipv4-family multicast** 命令删除 BGP 的 Ipv4 组播地址族视图下的所有配置

（续表）

步骤	命令	说明
10	**peer** *group-name* **enable** **例如：**[Huawei-bgp-af-multicast] **peer ex enable**	（可选）为指定 BGP 对等体组使能 MP-BGP 功能，使之成为 MP-BGP 对等体组（**具体使能的是哪种对等体组，要视本命令是在哪个地址族视图下配置的**）。命令中的 *group-name* 参数用来指定要使能 MP-BGP 功能的对等体组名称。**仅当需要在非 BGP-IPv4 单播地址族下建立 BGP 对等体组时才需要配置本步骤，因为 BGP-IPv4 单播地址族下的对等体组功能是缺省使能的** 缺省情况下，只有 BGP-IPv4 单播地址族的对等体是自动使能的，可用 **undo peer** *group-name* **enable** 命令去使能对应地址族下指定对等体组的 MP-BGP 功能

14.6.4 配置 BGP 引入路由

BGP 协议本身不发现路由，因此需要将位于本地设备 IP 路由表中的其他路由（如 IGP 路由等）**引入到 BGP 路由表中**，从而将这些路由在 AS 之内或 AS 之间通过 BGP 协议传播。BGP 协议支持通过以下两种方式引入路由。

① Import 方式：按协议类型将 RIP 路由、OSPF 路由、ISIS 路由等协议的路由引入 BGP 路由表中。为了保证引入的 IGP 路由的有效性，Import 方式还可以引入静态路由和直连路由。具体配置步骤如表 14-10 所示。

② Network 方式：**逐条将 IP 路由表中已经存在的路由**（可能是静态路由、直连路由，也可能是 RIP、OSPF、IS-IS 路由）引入到 BGP 路由表中，比 Import 方式更精确。具体配置步骤如表 14-11 所示。

【经验之谈】在 Network 路由引入方式中，如果在本地设备 IP 路由表中存在多条不同协议发现的到达同一目的网段的路由，则最终引入 BGP 路由表的将是它们之中最优的那条。对于不同协议发现的路由，它们是通过外部优先级的值进行比较的，优先级值越小，优先级越高，越能成为最终被引入 BGP 路由表中的路由。有关各种路由协议的外部优先级请参见第 10 章表 10-1。

表 14-10 通过 Import 方式引入路由的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要引入路由的对应的 IP 地址族视图。命令中的选项说明如下 ● **unicast**：二选一选项，进入 IPv4 单播视图，引入 IPv4 单播路由 ● **multicast unicast**：二选一选项，进入 IPv4 组播视图，引入 IPv4 组播路由 缺省情况下，进入 BGP-IPv4 单播地址族视图，可用 **undo ipv4-family** { **unicast** | **multicast** }命令删除 BGP 的相应 IP 地址族视图下的所有配置。如果希望取消缺省使能 IPv4 单播地址族功能，可以执行 **undo default ipv4-unicast** 命令

（续表）

步骤	命令	说明
4	**import-route** *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] * 例如：[Huawei-bgp-af-ipv4] **import-route rip** 1	配置 BGP 引入其他协议的路由（**但不包括各种缺省路由**）进入本地 BGP 路由表中。命令中的参数说明如下 ● *protocol*：指定要引入的路由的路由协议类型，可以选择 **direct**、**isis**、**ospf**、**rip**、**static**、**unr** ● *process-id*：可选参数，指定当引入 RIP、OSPF、IS-IS 协议路由时的对应进程号，取值范围为 1～65 535 的整数 ● **med** *med*：可多选参数，指定路由引入后的 MED 属性值，取值范围为 0～4 294 967 295 的整数。用于判断进入其他 AS 时的路由优先级 ● **route-policy** *route-policy-name*：可多选参数，指定用于过滤要引入和修改 MED 属性的路由的路由策略名称，1～40 个字符，不支持空格，区分大小写 【说明】本命令的路由引入比较粗，缺省情况下（即不使用 **route-policy** *route-policy-name* 参数过滤要引入的路由时）它是对同一类协议、同一进程下的所有路由都引入到 BGP 路由表中，不像下面将要介绍的在 Network 方式下使用 network 命令可以精确地指出要引入的路由 缺省情况下，BGP 未引入任何路由信息，可用 **undo import-route** *protocol* [*process-id*]命令删除指定的引入路由
5	**default-route imported** 例如：[Huawei-bgp-af-ipv4] **default-route imported**	（可选）将本地 IP 路由表中其他协议的缺省路由（包括静态缺省路由，以及 RIP、OSPF 缺省路由）引入本地 BGP 路由表中 如果需要在本地 IP 路由表中不存在缺省路由的情况下，而又需要向对等体（组）发布缺省路由，则需要使用 **peer default-route-advertise** 命令 缺省情况下，BGP 不将缺省路由引入 BGP 路由表中，可用 **undo default-route imported** 命令配置不将缺省路由引入到 BGP 路由表中

表 14-11　　通过 Network 方式引入路由的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast**|**multicast**} 例如：[Huawei-bgp] **ipv4-family unicast**	进入对应的 IP 地址族视图
4	**network** *ipv4-address* [*mask* | *mask-length*] [**route-policy** *route-policy-name*] 例如：[Huawei-bgp-af-ipv4] **network** 10.0.0.0 255.255.0.0	将 IP 路由表中的路由（**可以是各种路由**，最终引入的是哪种协议的路由要视路由的优先级而定）以静态方式加入到 BGP 路由表中，并发布给对等体。命令中的参数说明如下 ● *ipv4-address*：指定 BGP 发布的 IPv4 路由。如果存在到达同一网段多条不同协议的路由，**最终会从各路由协议的路由中选出的最优路由**

（续表）

步骤	命令	说明
4	**network** *ipv4-address* [*mask* | *mask-length*] [**route-policy** *route-policy-name*] 例如：[Huawei-bgp-af-ipv4] **network** 10.0.0.0 255.255.0.0	• *mask* | *mask-length*：可选参数，指定 BGP 发布的 IPv4 路由地址对应的子网掩码（选择二选一参数 *mask* 时）或子网掩码长度（选择二选一参数 *mask-length* 时），如果没有指定本参数，则按自然网段地址的掩码进行处理 • **route-policy** *route-policy-name*：指于用于过滤路由发布的路由策略名称，1～40 个字符，不支持空格，区分大小写 【说明】本命令用来发布精确匹配的路由。也就是说，**指定的目的地址和前缀长度必须与本地 IP 路由表中对应的表项完全一致，路由才能正确发布**。如果网络掩码没有指定，此路由将被按照自然网段精确匹配 缺省情况下，BGP 不将 IP 路由表中的路由以静态方式加入 BGP 路由表中，可用 **undo network** *ipv4-address* [*mask* | *mask-length*]命令删除指定的以静态方式加入 BGP 路由表中的路由

14.6.5 BGP 基本功能管理

配置好 BGP 基本功能后，可以使用以下 **display** 视图命令进行管理，以验证配置结果。

① **display bgp peer** [**verbose**]：查看所有 BGP 对等体的信息。

② **display bgp peer** *ipv4-address* { **log-info** | **verbose** }：查看指定 BGP 对等体的信息。

③ **display bgp routing-table** [*ipv4-address* [*mask* | *mask-length*]]：查看指定或所有 BGP 路由信息。

④ **display bgp group** [*group-name*]：查看指定或所有对等体组信息。

⑤ **display bgp multicast peer** [[*peer-address*] **verbose**]：查看指定或所有 MBGP 对等体的信息。

⑥ **display bgp multicast group** [*group-name*]：查看指定或所有 MBGP 对等体组的信息。

⑦ **display bgp multicast network**：查看 MBGP 发布的路由信息。

⑧ **display bgp multicast routing-table** [*ip-address* [*mask-length* [**longer-prefixes**] | *mask* [**longer-prefixes**]]]：查看指定或所有 MBGP 路由表信息。

14.6.6 BGP 基本功能配置示例

本示例的基本拓扑结构如图 14-19 所示，需要在所有 Router 间运行 BGP 协议（如果没有在系统视图下全局配置路由器 ID 的话，则需要专门在 BGP 视图下为设备配置由 BGP 路由使用的路由器 ID），其中 RouterA、RouterB 之间建立 EBGP 连接，RouterB、RouterC 和 RouterD 之间建立 IBGP 全连接。

1. 基本配置思路分析

本示例的要求很简单，仅需要在各路由器上启动 BGP 进程，然后根据要求在各路由器上配置 EBGP 或 IBGP 对等体，引入必要的路由即可。14.6.2 小节表 14-8 中的可选配

置均可不予配置。

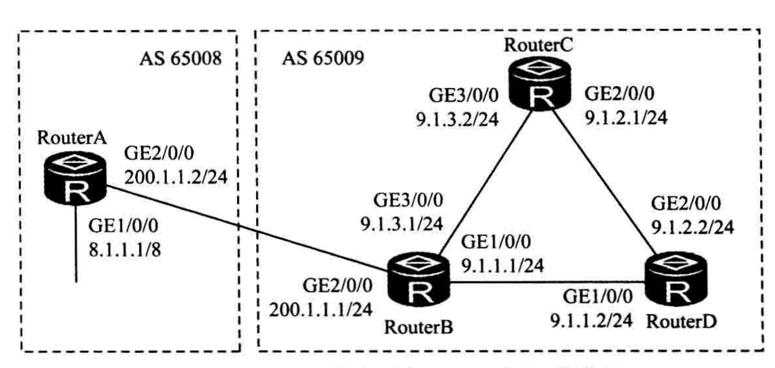


图 14-19　BGP 基本功能配置示例拓扑结构

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 8.1.1.1 8
```

② 配置 RouterB、RouterC 和 RouterD 之间的 IBGP 连接。注意，每个对等体连接均需要在双方设备上分别配置，且 IBGP 对等体中，双方都处于同一个 AS 中。因为本示例没有配置 Loopback 接口，也没有在系统视图下全局配置路由器 ID，所以需要在 BGP 视图下手动配置各路由器 ID。为了便于区分，RouterB、RouterC 和 RouterD 的路由器 ID 分别设为 2.2.2.2、3.3.3.3 和 4.4.4.4。此处，IBGP 连接的源接口和源 IP 地址均缺省采用设备的物理接口和物理接口 IP 地址。

RouterB 上的配置如下。

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 9.1.1.2 as-number 65009
[RouterB-bgp] peer 9.1.3.2 as-number 65009
```

RouterC 上的配置如下。

```
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 9.1.3.1 as-number 65009
[RouterC-bgp] peer 9.1.2.2 as-number 65009
```

RouterD 上的配置如下。

```
[RouterD] bgp 65009
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 9.1.1.1 as-number 65009
[RouterD-bgp] peer 9.1.2.1 as-number 65009
```

③ 配置 RouterA 与 RouterB 之间的 EBGP 连接，也需要在双方分别配置，此处也采用缺省的物理接口和物理接口 IP 地址作为 EBGP 连接源接口和源 IP 地址。RouterA 的路由器 ID 设为 1.1.1.1。

RouterA 上的配置如下。

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
```

```
[RouterA-bgp] peer 200.1.1.1 as-number 65009
```

RouterB 上的配置如下。

```
[RouterB-bgp] peer 200.1.1.2 as-number 65008
```

配置好 BGP 对等体后，可通过 **display bgp peer** 命令查看各设备上的 BGP 对等体的连接状态。下面是同时有 IBGP 连接和 EBGP 连接的 RouterB 上的输出结果，从中可以看出，RouterB 到其他路由器的 BGP 连接均已建立（**参见输出信息中的粗体字部分**）。

```
[RouterB] display bgp peer
 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 3                Peers in established state : 3
  Peer        V    AS   MsgRcvd  MsgSent  OutQ   Up/Down        State PrefRcv
  9.1.1.2     4 65009      49       62    0 00:44:58 Established     0
  9.1.3.2     4 65009      56       56    0 00:40:54 Established     0
  200.1.1.2   4 65008      49       65    0 00:44:03 Established     1
```

④ 配置 RouterA 发布与 EBGP 对等体之间的非直连路由 8.0.0.0/8。注意，这里要在对应的地址视图下进行配置，因为如果是在 BGP 视图下发布，将在多种地址族下生效。

```
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] network 8.0.0.0 255.0.0.0
```

此时可通过 **display bgp routing-table** 命令查看各路由器上的 BGP 路由表信息，可发现它们均已有 RouterA 发表的这条 8.0.0.0/8 路由，其中前面带*的路由表示有效路由。

下面分别是 RouterA、RouterB 和 RouterC 上的输出信息（RouterD 的路由信息与 RouterC 上的一样），从中可以看出，RouterA 和 RouterB 上的该路由都是有效的，而 RouterC 虽然学习到了 AS65008 中的 8.0.0.0/8 路由，但因为下一跳 200.1.1.2 不可达（**因为目前还没有 BGP 路由到达**），所以也不是有效路由。

```
[RouterA] display bgp routing-table
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.0.0.0            0.0.0.0         0                      0      i

[RouterB] display bgp routing-table
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.0.0.0            200.1.1.2      0                      0      65008i

[RouterC] display bgp routing-table
 BGP Local router ID is 3.3.3.3
```

```
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 i  8.0.0.0              200.1.1.2      0          100       0       65008i
```

【经验之谈】从以上路由表信息可以看到，RouterA 上的 8.0.0.0/8 路由的下一跳为 0.0.0.0，因为这条路由是本地设备上通告的，没有经过下一跳，而 RouterB 和 RouterC 上的 8.0.0.0/8 路由的下一跳均为 200.1.1.2，那是因为在 EBGP 对等体之间的 EBGP 路由发布时，下一跳将为发送路由器的出接口 IP 地址，**在 IBGP 对等体之间的 EBGP 路由发布时，下一跳不变**。而 IBGP 对等体之间进行 IBGP 路由发布时只能进行单跳通告，收到 IBGP 路由的设备不再通告给它自己的对等体。

在路由表中最后一列的“Path/Ogn”用来表示路由的 AS 路径和路由源类型，因为 8.0.0.0/8 路由是通过 **network** 命令通告的，所以显示为 i，代表 IGP 类型。

⑤ 为了解决 RouterC 和 RouterD 可以到达 8.0.0.0/8 路由的下一跳 200.1.1.2，只须在它们共同连接的 RouterB 上使 BGP 协议引入直连路由即可。配置如下。

```
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] import-route direct
```

此时可以看到，在 RouterA 的 BGP 路由表中除了有原来自己通告的 8.0.0.0/8 路由表项外，还有 RouterB 引入的三条直连路由，具体如下所示（**参见输出信息中的粗体字部分**），其中带>的表示到达对应网段的优选路由。

```
[RouterA] display bgp routing-table
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 4
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.0.0.0            0.0.0.0        0                    0       i
 *>   9.1.1.0/24         200.1.1.1      0                    0       65009?
 *>   9.1.3.0/24         200.1.1.1      0                    0       65009?
      200.1.1.0          200.1.1.1      0                    0       65009?
```

在 RouterC 的 BGP 路由表中也可见到 RouterB 所引入的三条直连路由，另外，原来的 8.0.0.0/8 路由变为有效、可达到了（前面有一个*号），具体如下所示（**参见输出信息中的粗体字部分**）。

```
[RouterC] display bgp routing-table
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 4
```

```
      Network        NextHop     MED      LocPrf   PrefVal  Path/Ogn

 *>i  8.0.0.0        200.1.1.2   0        100      0        65008i
 *>i  9.1.1.0/24     9.1.3.1     0        100      0        ?
  i   9.1.3.0/24     9.1.3.1     0        100      0        ?
 *>i  200.1.1.0      9.1.3.1     0        100      0        ?
```

14.6.7 MBGP 基本功能配置示例

本示例的基本拓扑结构如图 14-20 所示，接收者（Receiver）通过组播方式接收视频点播信息，接收者与组播源（Source）位于不同的 AS 中，现需要在两个 AS 之间传输组播路由信息。网络中各路由器接口 IP 地址如表 14-12 所示。

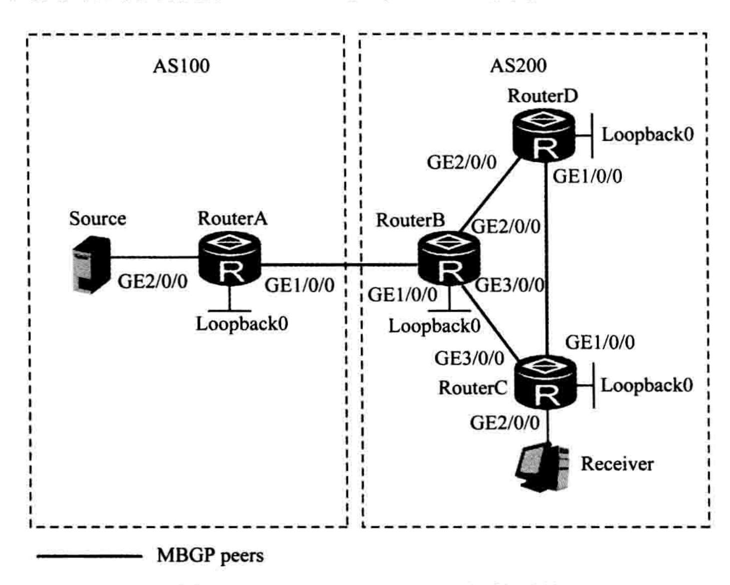


图 14-20 MBGP 配置示例拓扑结构

表 14-12 示例中各路由器接口 IP 地址

设备	接口	IP 地址	设备	接口	IP 地址
RouterA	GE1/0/0	10.1.1.1/24	RouterC	GE1/0/0	10.4.1.1/24
	GE2/0/0	10.10.10.1/24		GE2/0/0	10.168.1.1/24
	Loopback0	1.1.1.1/32		GE3/0/0	10.2.1.1/24
RouterB	GE1/0/0	10.1.1.2/24		Loopback0	3.3.3.3/32
	GE2/0/0	10.3.1.2/24	RouterD	GE1/0/0	10.4.1.2/24
	GE3/0/0	10.2.1.2/24		GE2/0/0	10.3.1.1/24
	Loopback0	2.2.2.2/32		Loopback0	4.4.4.4/32

1. 基本配置思路分析

本示例是一个组播 BGP 路由配置示例，且跨越两个 AS，主要有两个方面的配置：一是配置组播 BGP 路由，二是配置 IP 组播功能。在组播路由方面，AS200 内部可采用 OSPF 路由（当然也可以是其他路由协议）来实现 AS 内部 IBGP 对等体间的路由互通，然后在两个 AS 的边界路由器配置 EBGP 对等体连接，实现 AS 间的组播网络连接。由此可以得出本示例将涉及以下配置任务。

① 配置各路由器 IP 地址以及 AS200 内 RouterB、RouterC 和 RouterD 之间通过 OSPF 协议实现网络互通。

② 配置两个 AS 中各路由器的 MBGP 对等体，建立 AS 内、AS 间的组播路由。

③ 配置各路由器在 MBGP 视图下要引入的路由。

④ 使能各路由器的组播功能。

⑤ 在各 AS 内部配置 PIM-SM 基本功能，在主机侧接口上使能 IGMP 功能。

⑥ 在两个 AS 的 PIM 域间相连的接口上配置 BSR 服务边界。

⑦ 在两个 AS 的 PIM 域间边界路由器上配置 MSDP 对等体，实现传输域间组播源信息。

有关 IP 组播方面的配置请参见配套图书《华为交换机学习指南》。

2. 具体配置步骤

① 配置各路由器的接口 IP 地址以及 AS200 内三台路由器上的 OSPF 协议。注意，RouterB 的 GE1/0/0 接口上运行的不是 OSPF 协议，而是 EBGP 协议。

以下是 RouterA 上接口 IP 地址的配置，RouterB、RouterC 和 RouterD 上接口 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0]quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.10.10.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface loopback 0
[RouterA-loopback0] ip address 1.1.1.1 32
```

下面是 AS200 中各路由器的 OSPF 路由配置。因为没有划分区域，所以所有设备在骨干区域 0 中。

【经验之谈】 RIP、OSPF 和 IS-IS 协议中的 **network** 命令其实就是用来指定哪个接口上要运行对应的路由协议，然后以对应路由协议向邻居通告这些接口上所连接网络的路由信息。

RouterB 上的配置如下。

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.200] network 10.2.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.200] network 10.3.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.200] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.200] quit
```

RouterC 上的配置如下。

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.200] network 10.2.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.200] network 10.4.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.200] network 10.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.200] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.200] quit
```

RouterD 上的配置如下。

```
[RouterD] ospf
[RouterD-ospf-1] area 0
```

```
[RouterD-ospf-1-area-0.0.0.200] network 10.3.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.200] network 10.4.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.200] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.200] quit
```

② 在各路由器上使能 MBGP 协议，配置 MBGP 对等体。

注意 配置 MBGP 对等体前必须先在 BGP 视图下创建 BGP 对等体，然后在 BGP-IPv4 组播地址族下使能与 BGP 对等体交换组播路由信息的功能。因为创建 BGP 对等体后缺省只是使能 BGP-IPv4 单播地址族下与 BGP 对等体的路由信息交换功能，所以其他地址族下的该功能使能必须手动配置。

RouterA 上的配置如下。

```
[RouterA] bgp 100
[RouterA-bgp] peer 10.1.1.2 as-number 200
[RouterA-bgp] ipv4-family multicast
[RouterA-bgp-af-multicast] peer 10.1.1.2 enable
[RouterA-bgp-af-multicast] quit
[RouterA-bgp] quit
```

RouterB 上的配置如下。

```
[RouterB] bgp 200
[RouterB-bgp] peer 10.1.1.1 as-number 100
[RouterB-bgp] peer 10.2.1.1 as-number 200
[RouterB-bgp] peer 10.3.1.1 as-number 200
[RouterB-bgp] ipv4-family multicast
[RouterB-bgp-af-multicast] peer 10.1.1.1 enable
[RouterB-bgp-af-multicast] peer 10.2.1.1 enable
[RouterB-bgp-af-multicast] peer 10.3.1.1 enable
[RouterB-bgp-af-multicast] quit
[RouterB-bgp] quit
```

RouterC 上的配置如下。

```
[RouterC] bgp 200
[RouterC-bgp] peer 10.2.1.2 as-number 200
[RouterC-bgp] peer 10.4.1.2 as-number 200
[RouterC-bgp] ipv4-family multicast
[RouterC-bgp-af-multicast] peer 10.2.1.2 enable
[RouterC-bgp-af-multicast] peer 10.4.1.2 enable
[RouterC-bgp-af-multicast] quit
[RouterC-bgp] quit
```

RouterD 上的配置如下。

```
[RouterD] bgp 200
[RouterD-bgp] peer 10.3.1.2 as-number 200
[RouterD-bgp] peer 10.4.1.1 as-number 200
[RouterD-bgp] ipv4-family multicast
[RouterD-bgp-af-multicast] peer 10.3.1.2 enable
[RouterD-bgp-af-multicast] peer 10.4.1.1 enable
[RouterD-bgp-af-multicast] quit
[RouterD-bgp] quit
```

③ 在各路由器上配置要引入的路由，包括在 BGP 视图下引入的路由，用于 IPv4 单播通信（**当然，如果不需要进行 IPv4 单播通信也可不配置**）的路由以及在 IPv4 组播地址族下引入的路由，用于组播通信。

RouterA 上的配置如下。

因为 RouterA 与 RouterB 之间建立的是 EBGP 连接，所以必须要在组播地址族下引入 RouterA 上的直连路由，以便向 RouterB 通告其连接的直连路由，然后由 RouterB 在 AS200 内部通告，使得 AS200 中的所有设备可以访问到 RouterA 上连接的网络。

```
[RouterA] bgp 100
[RouterA-bgp] import-route direct   !---此配置可选，如果不需要进行 BGP-IPv4 单播通信就可不配置，下同
[RouterA-bgp] ipv4-family multicast
[RouterA-bgp-af-multicast] import-route direct
[RouterA-bgp-af-multicast] quit
[RouterA-bgp] quit
```

RouterB 上的配置如下。

同样，因为 RouterB 与 RouterA 之间建立的是 EBGP 连接，所以必须要在组播地址族下同时引入它的直连路由以及 AS200 内部的 OSPF 路由，以便向 RouterA 通告其直连路由和所学习到的 OSPF 路由，实现 RouterA 可以访问到 AS200 中所有设备的目的。因为直连路由的优先级高于 OSPF 路由，如果仅引入 OSPF 路由，则直连网段部分仍然无法实现互通。

```
[RouterB] bgp 200
[RouterB-bgp] import-route direct
[RouterB-bgp] import-route ospf 1 !---此配置可选，如果不需要进行 BGP-IPv4 单播通信就可不配置，下同
[RouterB-bgp] ipv4-family multicast
[RouterB-bgp-af-multicast] import-route direct
[RouterB-bgp-af-multicast] import-route ospf 1
[RouterB-bgp-af-multicast] quit
[RouterB-bgp] quit
```

RouterC 和 RouterD 上的路由引入配置与 RouterB 上的配置有些区别，因为它们上面均只需要在 AS200 内部进行组播通信，无需与外界进行 IPv4 单播 OSPF 通信，所以无需在 BGP-IPv4 单播地址族下引入 OSPF 路由，仅需在组播地址族下引入。但直连路由必须同时在 BGP-IPv4 单播地址族和组播地址族下分别引入，同样是因为直连路由的优先级高于 OSPF 路由。

```
[RouterC] bgp 200
[RouterC-bgp] import-route direct
[RouterC-bgp] ipv4-family multicast
[RouterC-bgp-af-multicast] import-route direct
[RouterC-bgp-af-multicast] import-route ospf 1
[RouterC-bgp-af-multicast] quit
[RouterC-bgp] quit
```

④ 使能各路由器及其相连接口的组播功能。同时，要在 RouterC 连接接收者主机的 GE2/0/0 接口上使能 IGMP 功能。

RouterA 上的配置如下。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] multicast routing-enable
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] pim sm
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] pim sm
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] pim sm
[RouterB-GigabitEthernet3/0/0] quit
```

RouterC 上的配置如下。

```
[RouterC] multicast routing-enable
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] pim sm
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] pim sm
[RouterC-GigabitEthernet2/0/0] igmp enable
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] pim sm
[RouterC-GigabitEthernet3/0/0] quit
```

RouterD 上的配置如下。

```
[RouterD] multicast routing-enable
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] pim sm
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] pim sm
[RouterD-GigabitEthernet2/0/0] quit
```

⑤ 在两个 PIM 域中分别配置 BSR 和 RP。BSR 位于 PIM 域边界，通常是把 BSR 与 RP 配置成一样。

RouterA 上的配置如下。

```
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.255
[RouterA-LoopBack0] pim sm
[RouterA-LoopBack0] quit
[RouterA] pim
[RouterA-pim] c-bsr loopback 0
[RouterA-pim] c-rp loopback 0
[RouterA-pim] quit
```

RouterB 上的配置如下。

```
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 2.2.2.2 255.255.255.255
[RouterB-LoopBack0] pim sm
[RouterB-LoopBack0] quit
[RouterB] pim
[RouterB-pim] c-bsr loopback 0
[RouterB-pim] c-rp loopback 0
[RouterB-pim] quit
```

在 AS100 和 AS200 这两个 PIM 域中配置域间相连接口为各自 PIM 域的 BSR 服务边界。

RouterA 上的配置如下。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim bsr-boundary
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] pim bsr-boundary
[RouterB-GigabitEthernet1/0/0] quit
```

⑥ 配置 MSDP 对等体。

因为 PIM 域间是通过 MSDP 服务进行连接的，所以在 PIM 域间的边界设备上要分别使能 MSDP 功能，并且要分别配置 MSDP 对等体。对等体就是对端接口的 IP 地址。

RouterA 上的配置如下。

```
[RouterA] msdp
[RouterA-msdp] peer 10.1.1.2 connect-interface gigabitethernet 1/0/0
[RouterA-msdp] quit
```

RouterB 上的配置如下。

```
[RouterB] msdp
[RouterB-msdp] peer 10.1.1.1 connect-interface gigabitethernet 1/0/0
[RouterB-msdp] quit
```

配置好以上内容后，可通过使用 **display bgp multicast peer** 命令查看两个 PIM 域边界路由器之间 MBGP 对等体的关系。以下是 RouterA 上 MBGP 对等体关系信息，RouterB 上的类似。

```
[RouterA] display bgp multicast peer
 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Total number of peers : 1                  Peers in established state : 1
  Peer          V    AS    MsgRcvd   MsgSent   OutQ   Up/Down        State        PrefRcv
  10.1.1.2      4   200       82        75       0 00:30:29   Established          17
```

也可使用 **display msdp brief** 命令查看路由器之间 MSDP 对等体建立情况。以下是 RouterB 上 MSDP 对等体关系，RouterA 上的类似。

```
[RouterB] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured      Up        Listen          Connect        Shutdown       Down
  1               1         0               0              0              0
  Peer's Address  State     Up/Down time    AS             SA Count       Reset Count
  10.1.1.1        Up        00:07:17        100            1              0
```

14.7　BGP 路由选路和负载分担配置与管理

BGP 具有很多路由属性（如 BGP 协议优先级、下一跳属性、本地优先级属性、AS 路径属性、MED 属性、团体属性等），而这些属性又可能影响 BGP 的最终选路结果。所以，本节涉及的配置任务比较多，具体如下。这些任务均为并列关系，用户可根据具体的应用环境和需求选择其中的一项或多项进行配置。在配置控制 BGP 的路由选择之前，需先配置 BGP 的基本功能。

① 配置 BGP 协议优先级。

② 配置 Next_Hop 属性。
③ 配置 BGP 路由首选值。
④ 配置本机缺省 Local_Pref 属性。
⑤ 配置 AS_Path 属性。
⑥ 配置 MED 属性。
⑦ 配置 BGP 团体属性。
⑧ 配置 BGP 负载分担。
下面各小节将分别介绍以上配置任务的具体配置方法。

14.7.1 配置 BGP 协议优先级

由于路由器上可能同时运行多个路由协议，就存在各个路由协议之间路由信息共享和路由路径选择的问题。系统为每一种路由协议设置一个缺省的内、外部优先级，具体参见第 10 章表 10-1 和表 10-2。在不同协议发现同一条路由时，优先级高的路由将被优选。

BGP 协议的外部优先级（这里包括 EBGP 优先级、IBGP 优先级和本地优先级三种）的具体配置步骤如表 14-13 所示。

表 14-13　　BGP 协议优先级配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置 BGP 协议优先级的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的协议优先级**
4	**preference** { *external internal local* | **route-policy** *route-policy-name* } 例如：[Huawei-bgp-af-ipv4] **preference** 2 2 20	配置 EBGP、IBGP、本地路由的协议优先级。命令中的参数说明如下 • *external*：指定 EBGP 路由（外部路由）的协议优先级。外部路由是从其他 AS 的对等体学来的最佳路由，取值范围为 1～255 的整数，值越小，优先级越高。本参数与下面的 *internal* 和 *local* 参数共同构成一个二选一参数 • *internal*：指定 IBGP 路由（内部路由）的协议优先级。内部路由是从同一个 AS 的对等体学来的路由，取值范围为 1～255 的整数，值越小，优先级越高 • *local*：指定 BGP 本地路由的协议优先级。本地路由是指通过聚合命令（**summary automatic** 自动聚合和 **aggregate** 手动聚合）所聚合的路由，取值范围为 1～255 的整数，值越小，优先级越高。有关 BGP 路由聚合将在本章后面具体介绍 • **route-policy** *route-policy-name*：二选一参数，指定用于配置 BGP 协议优先级的路由策略名称，1～40 个字符，区分大小写，不支持空格

（续表）

步骤	命令	说明
4	**preference** { *external internal local* | **route-policy** *route-policy-name* } 例如：[Huawei-bgp-af-ipv4] **preference** 2 2 20	【说明】使用路由策略配置 BGP 协议优先级的操作步骤如下（有关路由策略的具体配置方法将在本书第 15 章介绍） ① 使用 **route-policy** 命令创建 Route-Policy，并且进入 Route-Policy 视图 ② 配置 **if-match** 子句，为路由设置匹配条件。对于同一个 Route-Policy 节点，在匹配的过程中，各个 **if-match** 子句间是“与”的关系，即路由信息必须同时满足所有匹配条件，才可以执行 **apply** 子句的动作。如不指定 **if-match** 子句，则所有路由信息都会通过该节点的过滤 ③ 使用 **apply preference** 命令，为通过过滤的路由设定优先级 缺省情况下，EBGP、IBGP 和 BGP 本地路由的优先级均为 255，可用 **undo preference** 命令恢复优先级的缺省值

14.7.2　配置 Next_Hop 属性

BGP 在 Next_Hop 属性中规定，当 ASBR（连接 BGP 路由器的肯定是 ASBR）将从 EBGP 对等体学习到的路由转发给本 AS 内其他 IBGP 对等体时，**默认不修改下一跳**。这样一来，在 IBGP 对等体收到该路由后，会发现下一跳不可达（因为其下一跳不是直连设备的接口 IP 地址），于是将该路由设为非活跃路由，不通过该路由指导流量转发。

这时，如果希望 IBGP 邻居通过该路由指导流量转发，可以在 ASBR 上配置向 IBGP 对等体（组）转发路由时，将自身出接口 IP 地址作为下一跳。这样，IBGP 对等体在收到 ASBR 从 EBGP 邻居学习来的路由后发现下一跳可达，于是将路由设为活跃路由。

注意　当 BGP 路由发生变化时，BGP 需要对非直连的下一跳重新进行迭代。如果不对迭代后的路由进行任何限制，则 BGP 可能会将下一跳迭代到一个错误的转发路径上，从而造成流量丢失。此时，可配置 BGP 按路由策略迭代下一跳，避免流量丢失。

配置 BGP Next_Hop 属性的步骤如表 14-14 所示。

表 14-14　BGP Next_Hop 属性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置 BGP Next_Hop 属性的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的 Next_Hop 属性**
4	**peer** { *ipv4-address* | *group-name* } **next-hop-local** 例如：[Huawei-bgp-af-ipv4]**peer** 1.1.1.2 **next-hop-local**	（可选）配置 IBGP 设备向 **IBGP 对等体（组）发布来自 EBGP 对等体的路由时**，把下一跳地址设为自身的 IP 地址。命令中的 *ipv4-address* | *group-name* 参数分别用来指定对等体的 IP 地址或对等体组的名称

（续表）

步骤	命令	说明
4	**peer** { *ipv4-address* | *group-name* } **next-hop-local** 例如：[Huawei-bgp-af-ipv4]**peer** 1.1.1.2 **next-hop-local**	缺省情况下，IBGP 设备向 **IBGP 对等体发布来自 EBGP 对等体的路由时，不修改下一跳地址**，可用 **undo peer** { *ipv4-address* | *group-name* } **next-hop-local** 命令用来恢复发给指定对等体（组）的 EBGP 路由不改变下一跳
5	**nexthop recursive-lookup route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **nexthop recursive-lookup route-policy** rp_nexthop	（可选）配置 BGP 按路由策略对**从 IBGP 对等体收到的路由**进行下一跳迭代。命令中的参数 **route-policy** *route-policy-name* 用来指定进行下一跳迭代的路由策略的名称，1～47 个字符，区分大小写，不支持空格 【说明】可以利用路由策略来限制迭代后的路由，如果迭代后的路由不能通过指定路由策略的过滤，则将该路由标识为不可达。这样就能避免将非直连下一跳迭代到错误的转发路径上。执行该命令前，需要先确定允许被迭代到的路由，并配置相应的路由策略 **对于从直连 EBGP 对等体收到的路由，本命令不生效** 缺省情况下，BGP 不按路由策略进行下一跳迭代，可用 **undo nexthop recursive-lookup route-policy** 命令恢复缺省配置
6	**peer** { *group-name* | *ipv4-address* } **next-hop-invariable** **例如**：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **next-hop-invariable**	（可选）**在 IPv4 单播地址族下**配置发布引入的 IGP 路由时不改变该 IGP 路由的下一跳地址，参数 *group-name* | *ipv4-address* 分别指定要发布引入的 IGP 路由时的 IBGP 对等体组的名称和 IBGP 对等体的 IP 地址 【注意】在向 IBGP 对等体（组）通告路由时，本命令和前面介绍的 **peer next-hop-local** 命令互斥，不能同时配置 缺省情况下，对等体在发布所引入的 IGP 路由时会将下一跳地址改为本地与对端连接的接口地址，可用 **undo peer** { *ipv4-address* | *group-name* } **next-hop-invariable** 命令恢复为缺省配置

14.7.3 配置 BGP 路由首选值

协议首选值（PrefVal）是华为设备的私有属性，**仅在本地路由器上有效**。当 BGP 路由表中存在到达相同目的地址的多条路由时，将优先选择协议首选值高的路由（**而不管其他属性值**，因为首选属性值是最优先进行比较的，具体参见 14.5.1 小节）。

BGP 路由首选值的具体配置步骤如表 14-15 所示。

表 14-15　　BGP 路由首选值的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp]**ipv4-family unicast**	进入要配置 BGP 路由信息首选值的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的 BGP 路由信息首选值**

（续表）

步骤	命令	说明
4	**peer** { *group-name* | *ipv4-address* } **preferred-value** *value* 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **preferred-value** 50	为从指定对等体学来的所有路由配置首选值。但在为对等体分配首选值之前必须先配置 BGP 对等体。命令中的参数说明如下 ● *group-name* | *ipv4-address* 分别指定要设置首选值的路由所来自的 IBGP 对等体组的名称和 IBGP 对等体的 IP 地址 ● *value*：指定要为来自参数 *group-name* | *ipv4-address* 指定的对等组或对等体路由所分配的首选值，取值范围为 0～65 535 的整数，**值越大，优先级越高**。如果是对对等体组设置首选值，则对等体组里的每个对等体都继承这个配置 缺省情况下，从其他 BGP 对等体学来的路由的首选值为 0，可用 **undo peer** { *group-name* | *ipv4-address* } **preferred-value** 命令恢复来自指定对等体（组）的路由的首选值为缺省值

14.7.4　配置本机缺省 Local_Pref 属性

Local_Pref（本地优先级）属性用于判断流量**离开 AS 时的最佳路由**。当 BGP 的设备通过不同的 IBGP 对等体得到到达外部 AS 的目的地址相同，但下一跳不同的多条路由时，将优先选择 Local_Pref 属性值较高的路由。但 Local_Pref 属性**仅在 IBGP 对等体之间交换和比较，不通告给其他 AS。它表明的是 BGP 路由器的优先级，而不是路由的优先级。**

另外，因为 Local_Pref 属性是在上节介绍的 PrefVal 属性比较之后（具体参见 14.5.1 小节），所以仅当多条相同目的地址路由具有相同 PrefVal 属性值后才按 Local_Pref 属性值进行比较。

BGP 本地机缺省 Local_Pref 属性的具体配置步骤如表 14-16 所示。

表 14-16　BGP 本地机缺省 Local_Pref 属性的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置 Local_Pref 属性的对应 IP 地址族视图。**BGP 路由器在不同的地址族视图下可分别配置不同的 Local_Pref 属性值**
4	**default local-preference** *local-preference* 例如：[Huawei-bgp-af-ipv4] **default local-preference** 200	配置本地 BGP 路由器缺省的本地优先级属性值，其取值范围为 0～4 294 967 295 的整数，值越大，优先级越高 【注意】如果设备上已经配置了 BGP 的缺省本地优先级，当用户再次配置本地缺省优先级时，新的缺省优先级会取代原有的缺省优先级 缺省情况下，BGP 路由器的本地优先级的值为 100，可用 **undo default local-preference** 命令恢复 BGP 路由器的缺省本地优先级为缺省值

14.7.5 配置 AS_Path 属性

AS_Path（AS 路径）属性按矢量顺序记录了某条路由从本地到目的地址所要经过的所有 AS 编号。配置不同的 AS_Path 属性功能，可以实现灵活的路由选路。在配置 AS_Path 属性时，可以考虑以下几方面，可根据实际需要选择其中一项或多项进行配置，具体如表 14-17 所示。

① 通常情况下，将 AS_Path 属性内的 AS_Path 数量作为 BGP 选路条件，路径越长，优先级越低。当不需要 AS_Path 属性作为选路条件时，可以配置不将 AS_Path 属性作为选路条件。

② 通常情况下，BGP 通过 AS 号检测路由环路，即路由中的 AS 路径中包括本地 AS 号的路由不再接收。但在 Hub and Spoke 组网方式下，为保证路由能够正确传递，从 Hub-CE 发布私网路由到 Spoke-CE 途中经过的相关 BGP 对等体需要配置允许 AS_Path 中 AS 号重复一次的路由通过。

③ 公有 AS 号可以直接在 Internet 上使用，私有 AS 号直接发布到 Internet 上可能造成环路现象。为了解决上述情况，可以在把路由发布到 Internet 前，配置发送 EBGP 更新报文时，AS_Path 属性中仅携带公有 AS 编号。

④ 在重构 AS_Path 或聚合生成新路由时，可以对 AS_Path 中的 AS 号最大个数予以限制。配置 AS_Path 属性中 AS 号的最大个数后，接收路由时会检查 AS_Path 属性中的 AS 号是否超限，如果超限则丢弃路由。

⑤ 常规情况下，一个设备只支持一个 BGP 进程，即只支持一个 AS 号。但是在某些特殊情况下，例如网络由于迁移而更换 AS 号的时候，为了保证网络切换的顺利进行，可以为指定对等体设置一个伪 AS 号。

⑥ BGP 会检查 EBGP 对等体发来的更新消息中 AS_Path 列表的第一个 AS 号，确认第一个 AS 号必须是该 EBGP 对等体所在的 AS。否则，该更新信息被拒绝，EBGP 连接中断。如果不需要 BGP 检查 EBGP 对等体发来的更新消息中 AS_Path 列表的第一个 AS 号，可以去使能此功能。

表 14-17　AS_Path 属性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node* 例如：[Huawei] **route-policy policy permit node** 10	创建路由策略的节点，并进入路由策略视图（**有关路由策略的具体配置方法将在下章介绍**）。命令中的参数和选项说明如下 • *route-policy-name*：指定 Route-Policy 名称，1～40 个字符，区分大小写。如果该名称的路由策略不存在，则创建一个新的路由策略并进入它的路由策略视图。如果该名称的路由策略已经存在，则直接进入它的路由策略视图 • **deny**：二选一选项，指定路由策略节点的匹配模式为拒绝。如果路由与节点所有的 if-match 子句匹配成功，则该路由将被拒绝通过；否则进行下一节点 • **permit**：二选一选项，指定路由策略节点的匹配模式为拒绝。如果路由与节点所有的 **if-match** 子句匹配成功，则该路由将被拒绝通过；否则进行下一节点

（续表）

步骤	命令	说明
2	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node* 例如：[Huawei] **route-policy policy permit node** 10	• *node*：指定路由策略的节点号，取值范围为 0～65 535 的整数。当使用路由策略时，*node* 的值小的节点先进行匹配。一个节点匹配成功后，路由将不再匹配其他节点。全部节点匹配失败后，路由将被过滤 【说明】路由策略用于过滤路由信息以及为通过过滤的路由信息设置路由属性。一个路由策略由多个节点构成。一个节点包括多个 **if-match** 和 **apply** 子句。**if-match** 子句用来定义该节点的匹配条件，**apply** 子句用来定义通过过滤的路由行为。**if-match** 子句的过滤规则关系是“与”，即该节点的所有 **if-match** 子句都必须匹配。路由策略节点间的过滤关系是“或”，即只要通过了一个节点的过滤，就可通过该路由策略。如果没有通过任何一个节点的过滤，路由信息将无法通过该路由策略 缺省情况下，系统中没有路由策略，可用 **undo route-policy** *route-policy-name* [**node** *node*]命令删除指定的路由策略
3	（可选）配置路由策略匹配规则，只有满足匹配规则的路由才会改变 AS_Path 属性，有关路由策略的配置将在下章介绍。缺省情况下，所有路由都满足匹配规则。	
4	**apply as-path** { *as-number-plain* | *as-number-dot* } <1-10> { **additive** | **overwrite** } 例如：[Huawei-route-policy] **apply as-path** 200 10.10 **additive**	设置 BGP 路由的 AS_Path 属性，命令中的参数和选项说明如下 • *as-number-plain*：二选一参数，指定要替换或增加的整数形式的 AS 号，取值范围为 1～4 294 967 295 的整数。在同一个命令行中最多可以同时指定 10 个 AS 号 • *as-number-dot*：二选一参数，指定要替换或增加的点分形式的 AS 号，格式为 *x.y*，*x* 和 *y* 都是整数形式，*x* 的取值范围为 1～65 535 的整数，*y* 的取值范围为 0～65 535 的整数。在同一个命令行中最多可以同时指定 10 个 AS 号 • **additive**：二选一选项，指定要在路由的 AS 路径列表中添加指定的 AS 编号 • **overwrite**：二选一选项，用指定的 AS 号覆盖原有的 AS_Path 列表 【说明】配置此命令后，符合匹配条件的 BGP 路由的 AS_Path 列表将会改变。假设原来 AS_Path 为（30，40，50），在符合匹配条件的情况下 • 如果配置了 **apply as-path 60 70 80 additive** 命令，则 AS_Path 列表更改为（60，70，80，30，40，50）。这种配置一般用于调整使路由不被优选 • 如果配置了 **apply as-path 60 70 80 overwrite** 命令，则 AS_Path 列表更改为（60，70，80）。更改 AS_Path 的应用比较灵活，主要有以下几种情况。 ➢ 隐藏路由的真实路径信息。比如，AS_Path 列表更改为(60,70,80)之后，路由就丢失了原来携带的 AS_Path 路径信息（30，40，50） ➢ 用于形成负载分担。比如，设备收到两条路由，目的地址都是 10.1.0.0/16 这个网络，其中一条路由的 AS_Path 为（60，70，80），另一条路由的 AS_Path 为（30，40，50），如果把 AS_Path（30，40，50）更改为（60，70，80），那么这两条路由就有可能形成负载分担。

（续表）

步骤	命令	说明
4	**apply as-path** { *as-number-plain* | *as-number-dot* } &<1-10> { **additive** | **overwrite** } 例如：[Huawei-route-policy] **apply as-path** 200 10.10 **additive**	➢ 如果配置了 **as-path-limit** 命令，接收路由时会检查 AS_Path 属性中的 AS 号是否超限，如果超限则丢弃路由。这样对于 AS_Path 较长的路由，在接收之前，可以把 AS_Path 替换成较短的 AS_Path。例如原来的 AS_Path 为（60，70，80，65 001，65 002，65 003），可以配置 **apply as-path 60 70 80 overwrite** 命令，把 AS_Path 列表更改为（60，70，80），缩短 AS_Path 的长度，防止路由由于 AS 号超限而被丢弃 ➢ 缩短 AS_Path 长度，使路由被优选，把流量引导向本自治系统 ● 如果配置了 **apply as-path none overwrite** 命令，则 AS_Path 列表更改为空。BGP 在选路时，如果 AS_Path 列表为空，AS_Path 长度按照 0 来处理。通过清空 AS_Path，不但可以隐藏真实的路径信息，还可以缩短 AS_Path 长度，使路由被优选，把流量引导向本自治系统 缺省情况下，路由策略中未配置改变 BGP 路由的 AS_Path 属性的动作，可用 **undo apply as-path** 命令恢复缺省配置
5	**quit**	退出路由策略视图，返回系统视图
6	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
7	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp]**ipv4-family unicast**	进入要配置 AS_Path 属性的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的 AS_Path 属性值**
以下 8～11 的配置任务是并列关系，可根据实际需要选择配置其中的一项或几项		
8	**peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **export**	通过路由策略对向对等体(组)发布的路由配置指定 AS_Path 属性。命令中的参数说明如下 ● *ipv4-address* | *group-name*：分别用来指定对等体的 IP 地址或对等体组的名称 ● *route-policy-name*：指定用于为向指定的对等体或对等体组发布的路由配置 AS_Path 属性的路由策略 缺省情况下，对向对等体（组）发布的路由不使用路由策略配置 AS_Path 属性，可用 **undo peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export** 命令删除对向指定的对等体（组）发布的路由使用指定的路由策略配置 AS_Path 属性，恢复为缺省配置
9	**peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **import**	通过路由策略对从对等体(组)接收的路由配置指定 AS_Path 属性。命令中的参数说明如下 ● *ipv4-address* | *group-name*：分别用来指定对等体的 IP 地址或对等体组的名称 ● *route-policy-name*：指定用于从指定的对等体或对等体组接收的路由配置 AS_Path 属性的路由策略 缺省情况下，对来自对等体（组）发布的路由不使用路由策略配置 AS_Path 属性，可用 **undo peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* import 命令删除对来自指定的对等体（组）的路由使用指定的路由策略配置 AS_Path 属性，恢复为缺省配置

（续表）

步骤	命令	说明
10	**import-route** *protocol* [*process-id*] **route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **import-route rip** 1 **route-policy** test-policy	通过路由策略对在 BGP 路由器上以 Import 方式引入的路由配置指定的 AS_Path 属性。命令中的参数说明如下 ● *protocol*：指定要配置 AS_Path 属性的引入路由协议和路由类型，支持 **direct**、**isis**、**ospf**、**rip**、**static**、**unr** ● *process-id*：可选参数，指定要配置 AS_Path 属性的路由进程，仅当参数 *protocol* 为 **isis**、**ospf**、**rip** 时选择，取值范围为 1～65 535 的整数 ● *route-policy-name*：指定用于定义配置 AS_Path 属性的路由策略 缺省情况下，BGP 未引入任何路由信息，可用 **undo import-route** *protocol* [*process-id*]命令恢复缺省配置
11	**network** *ipv4-address* [*mask* | *mask-length*] **route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **network** 10.0.0.0 255.255.0.0 **route-policy** test-policy	通过路由策略对在 BGP 路由器上以 Network 方式静态引入的路由配置指定的 AS_Path 属性。命令中的参数说明如下 ● *ipv4-address*：指定引入的路由的网络地址 ● *mask* | *mask-length*：可选参数，指定引入的路由的子网掩码或子网掩码长度，如果不指定，则采用对应的自然网段子网掩码 ● *route-policy-name*：指定用于定义配置 AS_Path 属性的路由策略名称 缺省情况下，BGP 不将 IP 路由表中的路由以静态方式加入 BGP 路由表中，可用 **undo network** *ipv4-address* [*mask* | *mask-length*]命令删除指定的以静态方式加入 BGP 路由表中的路由
以下 12～14 的配置任务是并列关系，一般为可选配置任务，可根据实际需要选择配置其中的一项或几项		
12	**bestroute as-path-ignore** 例如：[Huawei-bgp-af-ipv4] **bestroute as-path-ignore**	（可选）配置 BGP 在选择最优路由时忽略 AS 路径属性 缺省情况下，BGP 将 AS 路径属性作为选择最优路由的一个条件，长度较小者优先，可用 **undo bestroute as-path-ignore** 命令恢复缺省配置
13	**peer** { *group-name* | *ipv4-address* } **allow-as-loop** [*number*] 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **allow-as-loop** 2	（可选）配置允许在从对等体（组）接收的路由的 AS_Path 列表中本地 AS 编号重复出现。命令中的参数说明如下 ● *ipv4-address* | *group-name*：指定要对来自指定的对等体或对等体组的路由配置允许本地 AS 号重复出现 ● *number*：可选参数，指定在路由的 AS_Path 列表中允许本地 AS 号的重复次数，取值范围为 1～10 的整数，缺省值为 1 【注意】本命令是覆盖式的，对于同一个对等体或对等体组，后一次配置会覆盖前一次的配置 缺省情况下，在收到的路由中不允许本地 AS 号重复，可用 **undo peer** { *group-name* | *ipv4-address* } **allow-as-loop** 命令恢复接收指定对等体（组）的路由中不允许本地 AS 号重复
14	**peer** { *group-name* | *ipv4-address* } **public-as-only** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **public-as-only**	（可选）配置向对等体（组）发送 BGP 更新报文时 AS_Path 属性不携带私有 AS 号，仅携带公有 AS 号。命令中的 *ipv4-address* | *group-name* 参数指定要对向指定对等体或对等体组发布路由更新报文时 AS_Path 属性不携带私有 AS 号 【注意】以下两种情况，配置本命令后 BGP 也不会删除私有 AS 号 ● 路由的 AS_Path 属性中含有对端的 AS 号时。这种情况下删除私有 AS 号，可能会造成路由环路

（续表）

步骤	命令	说明
14	**peer** { *group-name* | *ipv4-address* } **public-as-only** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **public-as-only**	• AS_Path 列表中同时含有公有 AS 号和私有 AS 号。该列表表明路由已经经过了公网，如果删除私有 AS 号，可能会造成转发错误 缺省情况下，发送 BGP 更新报文时，AS_Path 属性可以同时携带私有 AS 号和公有 AS 号，可用 **undo peer** { *group-name* | *ipv4-address* } **public-as-only** 命令向指定对等体（组）发布路由更新时可以同时携带私有 AS 号和公有 AS 号
15	**quit** 例如：[Huawei-bgp-af-ipv4] **quit**	退出地址族视图，返回 BGP 视图
以下 16～18 的配置任务是并列关系，一般为可选配置任务，可根据实际需要选择配置其中的一项或几项		
16	**as-path-limit** *as-path-limit-num* 例如：[Huawei-bgp] **as-path-limit** 200	（可选）配置 AS_Path 属性中 AS 号的最大个数，取值范围为 1～2 000 的整数，缺省值是 255 缺省情况下，AS_Path 属性中 AS 号的最大限制值是 2 000，可用 **undo as-path-limit** 命令恢复 AS_Path 属性中 AS 号的最大个数的缺省值
17	**peer** { *ipv4-address* | *group-name* } **fake-as** { *as-number-plain* | *as-number-dot* } 例如：[Huawei-bgp] **peer** 1.1.1.2 **fake-as** 100.200	（可选）配置指定 **EBGP 对等体**采用伪 AS 编号与本端建立连接。命令中的参数说明如下 • *ipv4-address* | *group-name*：指定要配置伪 AS 号的对等体的 IP 地址或对等体组的名称 • *as-number-plain*：二选一参数，指定整数形式的伪 AS 号，取值范围为 1～4 294 967 295 的整数 • *as-number-dot*：二选一参数，指定点分形式的伪 AS 号，格式为 *x.y*，*x* 和 *y* 都是整数形式，*x* 的取值范围为 1～65 535 的整数，*y* 的取值范围是 0～65 535 的整数 【说明】本命令常用于运营商修改网络部署的场景。例如当运营商 A 收购了运营商 B 时，由于两者位于不同的 AS，因此需要把运营商 B 的 AS 合并到运营商 A 的 AS 中，即将原运营商 B 的 AS 号修改为运营商 A 的 AS 号。但是在网络合并过程中，原运营商 B 位于其他 AS 的 BGP 对等体可能不期望或者不便立即修改本地的 BGP 配置，此时就会造成与这些对等体的连接中断 为了保证网络合并的顺利进行，可以在原运营商 B 的 ASBR 上执行 peer fake-as 命令，将原运营商 B 的 AS 号设置为合并后的运营商 A 的伪 AS 号，使原运营商 B 的 BGP 对等体能够继续使用伪 AS 号建立连接 缺省情况下，对等体使用真实的 AS 号与本端建立连接，可用 **undo peer** { *group-name* | *ipv4-address* } **fake-as** 命令恢复使用真实的 AS 号与本端建立连接
18	**undo check-first-as** 例如：[Huawei-bgp] **undo check-first-as**	（可选）取消检查 EBGP 对等体发来的更新消息中 AS_Path 属性的第一个 AS 号 【注意】配置本命令后产生环路的可能性增大，请慎重使用 缺省情况下，BGP 会检查 EBGP 对等体发来的更新消息中 AS_Path 列表的第一个 AS 号，确认第一个 AS 号必须是该 EBGP 对等体所在的 AS。否则，该更新信息被拒绝，EBGP 连接中断，可用 **check-first-as** 命令使能检查 EBGP 对等体发来的更新消息中 AS_Path 属性的第一个 AS 号的功能

14.7.6 配置 MED 属性

MED 属性相当于 IGP 使用的度量值（Metrics），它用于判断流量进入 AS 时的最佳路由。当一个运行 BGP 的设备通过不同的 EBGP 对等体得到目的地址相同但下一跳不同的多条路由时，在其他条件相同的情况下，**将优先选择 MED 值较小者作为进入 EBGP 对等体所有 AS 的最优路由。**

MED 属性的具体配置步骤如表 14-18 所示（**需在 EBGP 设备上配置**）。

表 14-18　MED 属性的具体配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node* 例如：[Huawei] **route-policy policy permit node** 10	创建路由策略的节点，并进入路由策略视图。命令中的参数和选项说明参见 14.7.5 小节表 14-16 中的第 2 步
3	（可选）配置路由策略匹配规则，只有满足匹配规则的路由才会改变 MED 属性，有关路由策略的配置将在下章介绍。缺省情况下，所有路由都满足匹配规则。	
4	**apply cost** [+ | -] *cost* 例如：[Huawei-route-policy] **apply cost** 120	在路由策略中配置改变路由的开销值（**在 BGP 中就是 MED 属性值**）的动作。命令中的参数和选项说明如下 ● +：二选一可选项，指定在路由的原路由开销基础上增加由 *cost* 参数指定的开销值。如果不指定+和-可选项，则表示用由 *cost* 参数指定的开销值替换路由的原路由开销值 ● −：二选一可选项，指定在路由的原路由开销基础上减少由 *cost* 参数指定的开销值。如果不指定+和-可选项，则表示用由 *cost* 参数指定的开销值替换路由的原路由开销值 ● *cost*：指定要增加，或者减少，或者用来替换原路由开销值的路由开销值，取值范围为 0～4 294 967 295 的整数 缺省情况下，在路由策略中未配置改变路由的开销值的动作，可用 **undo apply cost** 命令恢复缺省配置
5	**quit** 例如：[Huawei-route-policy] **quit**	退出路由策略视图，返回系统视图
6	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
7	**ipv4-family**{ **unicast** | **multicast**} 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置 MED 属性的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的 MED 属性值**
以下 8～12 的配置任务是并列关系，可根据实际需要选择配置其中的一项或几项		
8	**default med** *med* 例如：[Huawei-bgp-af-ipv4] **default med** 10	（可选）配置本地 BGP 路由的缺省 MED 值（本地所有没有专门配置 MED 属性值的 BGP 路由具有相同的 MED 属性值），取值范围为 0～4 294 967 295 的整数 【注意】MED 值仅在相邻两个 AS 之间传递，收到此属性的 AS 一方不会再将其通告给任何其他第三方 AS。如果设备上已经配置了 BGP 的缺省 MED 值，当用户再次配置缺省 MED 值时，新的缺省 MED 值会取代原有的缺省 MED 值 缺省情况下，MED 的值为 0，可用 **undo default med** 命令恢复缺省设置

（续表）

步骤	命令	说明
9	**bestroute med-none-as-maximum** 例如：[Huawei-bgp-af-ipv4] **bestroute med-none-as-maximum**	（可选）配置 BGP 在选择最优路由时，如果路由属性中没有 MED 属性值，则把 MED 属性值按最大值 4 294 967 295（优先级最低）来处理 缺省情况下，BGP 在选择最优路由时，如果路由属性中没有 MED 值，则按 0 处理，可用 **undo bestroute med-none-as-maximum** 命令恢复缺省设置
10	**compare-different-as-med** 例如：[Huawei-bgp-af-ipv4] **compare-different-as-med**	（可选）配置允许比较来自不同自治系统中的邻居的路由的 MED 值 【说明】本命令主要应用于控制 MED 属性改变 BGP 的选路策略。通过配置此命令可以允许 BGP 比较来自不同 AS 的路由的 MED 属性值。如果到达同一目的地址有多条可选有效路径，可以选择 MED 参数较小的路由作为最终实际使用的路由项。**但除非能够确认不同的自治系统采用了同样的 IGP 和路由选择方式，否则不要使用本命令** 缺省情况下，不允许比较来自不同 AS 邻居的路由路径的 MED 属性值，可用 **undo compare-different-as-med** 命令禁止比较来自不同 AS 邻居的路由路径的 MED 属性值
11	**deterministic-med** 例如：[Huawei-bgp-af-ipv4] **deterministic-med**	（可选）使能 BGP deterministic-med 功能，使在路由选路时优先比较 AS_Path 最左边的 AS 号（也就是离本地设备最近一个 AS）相同的路由 【说明】使能 deterministic-med 功能后，在对众多个不同 AS 收到的相同前缀的路由进行选路时，首先会按路由的 AS_Path 最左边的 AS 号进行分组。在组内进行比较后，再用组中的优选路由和其他组中的优选路由进行比较，消除了选路的结果和路由接收顺序的相关性 例如：假设在某台路由器上存在如下三条 BGP 路由 ● Route A1: AS(PATH) 12, med 100, igp metric 13, internal, rid 4.4.4.4 ● Route A2: AS(PATH) 12, med 150, igp metric 11, internal, rid 5.5.5.5 ● Route B: AS(PATH) 3, med 0, igp metric 12, internal, rid 6.6.6.6 此时，当路由收来的顺序为：Route A1、Route A2、Route B 时，先比较 A1、A2。因为 Route A1、Route A2 的最左 AS 相同，所以优选 MED 较小的路由 Route A1。再比较 Route A1 和 Route B，因为 Route A1、Route B 的最左 AS 不相同，在没有配置本命令情况下，不能比较 MED。优选 IGP Metric 较小的路由 Route B 当路由收来的顺序为：Route A2、Route B、Route A1 时，先比较 Route A2、Route B，因为 Route B 和 Route A2 的最左 AS 不相同，在未配置本命令情况下，优选 IGP Metric 较小的路由 Route A2。再比较 Route A2、Route A1，因为 Route A2 和 Route A1 的最左 AS 相同，所以优选 MED 较小的路由 Route A1 从上面的分析可以看到，没有使能 **deterministic-med** 功能时，最终优选的路由和路由接收的顺序相关。而使能了 **deterministic-med** 功能后，就会消除选路的结果和路由接收顺序的相关性。由于 Route A1、Route A2 的 AS_Path 最左边的 AS 号相同，所以无论路由接收顺序如何，都优先比较 Route A1、Route A2

（续表）

步骤	命令	说明
11	**deterministic-med** 例如：[Huawei-bgp-af-ipv4] **deterministic-med**	缺省情况下，deterministic-med 功能未使能，BGP 会按照路由接收的顺序依次进行比较，最终选路的结果和路由的接收顺序是相关的，可用 **undo deterministic-med** 命令去使能 deterministic-med 功能，优先比较先接收的路由
12	**bestroute med-confederation** 例如：[Huawei-bgp-af-ipv4] **bestroute med-confederation**	（可选）配置 BGP 在选择最优路由时，仅在联盟内比较 MED 属性值 【说明】在缺省情况下，BGP 只比较来自同一 AS 的路由的 MED 值。这里的 AS 不包括联盟的子 AS。为了使 BGP 在联盟内选择最优路由时能够比较 MED 值，可以配置本命令。配置本命令后，只有当 AS_Path 中不包含外部 AS（不在联盟内的子 AS）号时才比较 MED 值的大小。如果 AS_Path 中包含外部 AS 号，则不进行比较 例如：自治系统 65000、65001、65002 和 65004 属于同一联盟。4 条到达同一目的地址的待选路由如下所示 • path1：AS_Path=65000 65004，med=2 • path2：AS_Path=65001 65004，med=3 • path3：AS_Path=65002 65004，med=4 • path4：AS_Path=65003 65004，med=1 在配置本命令后，因为 path1、path2 和 path3 的 AS_Path 中不包含同一联盟外的自治系统，所以当 BGP 需要通过比较 MED 值来选择路由时，将只比较 path1、path2 和 path3 的 MED 值。而 path4 的 AS_Path 中包含同一联盟外的自治系统，因此不比较 path4 的 MED 值 缺省情况下，BGP 仅比较来自同一 AS 的路由的 MED 值，可用 **undo bestroute med-confederation** 命令恢复缺省配置
以下 13～16 的配置任务是并列关系，可根据实际需要选择配置其中的一项或几项		
13	**peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **export**	（可选）通过路由策略对向对等体（组）发布的路由配置指定 MED 属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 8 步，**只不过这里配置的是 MED 属性** 缺省情况下，对向对等体（组）发布的路由不使用路由策略配置 MED 属性，可用 **undo peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export** 命令删除对向指定的对等体（组）发布的路由使用指定的路由策略配置 MED 属性，恢复为缺省配置
14	**peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **import**	通过路由策略对从对等体（组）接收的路由配置指定 MED 属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 9 步，**只不过这里配置的是 MED 属性** 缺省情况下，对来自对等体（组）发布的路由不使用路由策略配置团体属性，可用 **undo peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **import** 命令删除对来自指定的对等体（组）的路由使用指定的路由策略配置 MED 属性，恢复为缺省配置
15	**import-route** *protocol* [*process-id*] **route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **import-route rip** 1 **route-policy** test-policy	通过路由策略在 BGP 以 import 方式引入路由时对引入的路由配置指定 MED 属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 10 步，**只不过这里配置的是 MED 属性** 缺省情况下，BGP 未引入任何路由信息，可用 **undo import-route** *protocol* [*process-id*]命令恢复缺省配置

（续表）

步骤	命令	说明
16	**network** *ipv4-address* [*mask* | *mask-length*] **route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **network** 10.0.0.0 255.255.0.0 **route-policy** test-policy	通过路由策略在BGP以network方式静态引入路由时对引入的路由配置指定 MED 属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 11 步，**只不过这里配置的是 MED 属性** 缺省情况下，BGP 不将 IP 路由表中的路由以静态方式加入BGP 路由表中，可用 **undo network** *ipv4-address* [*mask* | *mask-length*]命令删除指定的以静态方式加入 BGP 路由表中的路由

14.7.7 配置 BGP 团体属性

团体属性可在 BGP 对等体之间传播，且不受 AS 的限制。利用团体属性可以使多个 AS 中的一组 BGP 设备共享相同的策略，从而简化路由策略的应用并降低维护管理的难度。BGP 设备可以在发布路由时，新增或者改变路由的团体属性。由团体属性延伸的扩展团体属性是针对特定业务的扩展，目前仅支持在 VPN 中应用 Route-Target 属性。

BGP 团体属性的具体配置步骤如表 14-19 所示。

表 14-19　　BGP 团体属性的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node* 例如：[Huawei] **route-policy policy permit node** 10	创建路由策略的节点，并进入路由策略视图。命令中的参数和选项说明参见 14.7.5 小节表 14-17 中的第 2 步
3	（可选）配置路由策略匹配规则，只有满足匹配规则的路由才会改变团体属性，有关路由策略的配置将在下章介绍。缺省情况下，所有路由都满足匹配规则。	
4	**apply community** { *community-number* | *aa:nn* | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } &<1-32> [**additive**] 例如：[Huawei-route-policy] **apply community** 100 150	（二选一）配置 BGP 路由信息的团体属性。命令中的参数和选项说明如下。 ● *community-number*：多选一参数，指定要替换或追加的整数形式团体属性的团体号，取值范围为 0～4 294 967 295 的整数 ● *aa:nn*：多选一参数，指定要替换或追加的冒号分隔形式团体属性的团体号，其中 *aa* 代表主团体号，*nn* 代表子团体号，它们的取值范围都为 0～65 535 的整数 ● **internet**：多选一选项，表示符合路由策略条件的路由为可以向任何对等体发送的路由。缺省情况下，所有的路由都属于 Internet 团体 ● **no-advertise**：多选一选项，表示符合路由策略条件的路由为不能向任何对等体发送的路由。**即收到具有此属性的路由后，不能发布给任何其他的 BGP 对等体** ● **no-export**：多选一选项，表示符合路由策略条件的路由为不能向 AS 外发送的路由，但可以发布给联盟中的其他子 AS。**即收到具有此属性的路由后，不能发布到本地 AS 之外** ● **no-export-subconfed**：多选一选项，表示符合路由策略条件的路由为既不能向 AS 外发送的路由，也不能发布给联盟的其他子 AS 的路由。即收到具有此属性的路由后，不能发布给任何其他 AS 和子 AS

（续表）

步骤	命令	说明
4	**apply community** { *community-number* | *aa:nn* | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } &<1-32> [**additive**] 例如：[Huawei-route-policy] **apply community** 100 150	• &<1-32>：表示前面的这些多选一参数或选项在本条命令中最多可以配置 32 个 • **additive**：可选项，表示要向符合路由策略条件的路由追加指定的团体属性。如果没有此可选项，则表示替换原有的团体属性 【说明】在本命令中最多可以配置 32 个整数形式和冒号分隔形式的团体号。但这两种团体号具体可配置的数量要依据以下规则 • 如果不配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 选项，则 *community-number* 和 *aa:nn* 一共可以指定 32 个 • 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的一个选项，则 *community-number* 和 *aa:nn* 一共可以指定 31 个 • 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的两个选项，则 *community-number* 和 *aa:nn* 一共可以指定 30 个 • 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的三个选项，则 *community-number* 和 *aa:nn* 一共可以指定 29 个 • 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 选项，则 *community-number* 和 *aa:nn* 一共可以指定 28 个 缺省情况下，在路由策略中未配置改变 BGP 路由团体属性的动作，可用 **undo apply community** 命令用来恢复缺省配置。可用 **apply community none** 命令删除 BGP 路由的团体属性
	apply extcommunity { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address:nn* } } &<1-16> [**additive**] 例如：[Huawei-route-policy] **apply extcommunity rt** 100:2 **rt** 1.1.1.1:22 **rt** 100.100:100 **additive**	（二选一）配置 BGP 扩展团体属性（Route-Target）。命令中的参数和选项说明如下 • **rt**：指定对符合路由策略条件的路由替换或者追加扩展团体，最多可设置 16 个 • *as-number:nn*：多选一参数，指定带 2 字节 AS 号的扩展团体属性值，其中 *as-number* 为整数形式的 2 字节 AS 号，取值范围为 0～65 535 的整数，*nn* 为一个整数，取值范围为 0～4 294 967 295 • *4as-number:nn*：多选一参数，指定带 4 字节 AS 号的扩展团体属性值，其中 *4as-number* 为整数形式的 4 字节 AS 号。它有两种表示形式：（1）整数形式的取值范围为 65 536～4 294 967 295；（2）点分形式，格式为 *x.y*，*x* 和 *y* 都是整数形式，取值范围都为 0～65 535。*nn* 为一个整数，取值范围为 0～65 535 • *ipv4-address:nn*：多选一参数，指定 IP 地址点分格式的扩展团体属性值，其中 *ipv4-address* 为点分十进制形式的 IP 地址；*nn* 为一个整数，取值范围为 0～65 535 • &<1-16>：表示在本条命令中以上多选一参数，rt 关键字最多可配置 16 个

（续表）

步骤	命令	说明
4	**apply extcommunity** { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address:nn* } } &<1-16> [**additive**] 例如：[Huawei-route-policy] **apply extcommunity rt** 100:2 **rt** 1.1.1.1:22 **rt** 100.100:100 **additive**	• **additive**：可选项，表示要向符合路由策略条件的路由追加指定的扩展团体属性。如果没有此可选项，则表示替换原有的扩展团体属性 缺省情况下，在路由策略中未配置改变 BGP 路由的扩展团体属性的动作，可用 **undo apply extcommunity** 命令恢复缺省配置
5	**quit**	退出路由策略视图，返回系统视图
6	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
7	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置团体属性的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的团体属性值**
以下 8～11 的配置任务是并列关系，可根据实际需要选择配置其中的一项或几项		
8	**peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **export**	（可选）通过路由策略对向对等体（组）发布的路由配置指定团体属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 8 步，**只不过这里添加的是团体属性** 缺省情况下，对向对等体（组）发布的路由不使用路由策略添加团体属性，可用 **undo peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **export** 命令删除对向指定的对等体（组）发布的路由使用指定的路由策略配置团体属性，恢复为缺省配置
9	**peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **import**	（可选）通过路由策略对从对等体（组）接收的路由配置指定团体属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 9 步，**只不过这里添加的是团体属性** 缺省情况下，对来自对等体（组）的路由不使用路由策略配置团体属性，可用 **undo peer** { *ipv4-address* | *group-name* } **route-policy** *route-policy-name* **import** 命令删除对来自指定的对等体（组）的路由使用指定的路由策略配置团体属性，恢复为缺省配置
10	**import-route** *protocol* [*process-id*] **route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **import-route rip** 1 **route-policy** test-policy	（可选）通过路由策略对以 Import 方式引入的路由配置指定团体属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 10 步，**只不过这里添加的是团体属性** 缺省情况下，BGP 未引入任何路由信息，可用 **undo import-route** *protocol* [*process-id*]命令恢复缺省配置
11	**network** *ipv4-address* [*mask* | *mask-length*] **route-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **network** 10.0.0.0 255.255.0.0 **route-policy** test-policy	（可选）通过路由策略对以 Network 方式静态引入的路由配置指定团体属性。命令中的参数说明参见 14.7.5 小节表 14-17 中的第 11 步，**只不过这里添加的是团体属性** 缺省情况下，BGP 不将 IP 路由表中的路由以静态方式加入到 BGP 路由表中，可用 **undo network** *ipv4-address* [*mask* | *mask-length*]命令删除指定的以静态方式加入 BGP 路由表中的路由
以下是一个二选一选项，仅在需要对向对等体（组）发布的路由添加团体属性或者扩展团体属性时配置，其他情况不必配置		

（续表）

步骤	命令	说明
12	**peer** { *ipv4-address* | *group-name* } **advertise-community** 例如：[Huawei-bgp-af-ipv4] **bestroute as-path-ignore**	（二选一）配置允许将团体属性传给对等体或对等体组。参数 *ipv4-address* | *group-name* 用来把传递团体属性到指定的对等体或对待体组 缺省情况下，不将团体属性发布给任何对等体或对等体组，可用 **undo peer** { *ipv4-address* | *group-name* } **advertise-community** 命令恢复缺省配置
	peer { *ipv4-address* | *group-name* | *ipv6-address* } **advertise-ext-community** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **allow-as-loop** 2	（二选一）配置允许将扩展团体属性传给对等体或对等体组。参数 *ipv4-address* | *group-name* 用来把传递扩展团体属性到指定的对等体或对等体组 缺省情况下，不将扩展团体属性发布给任何对等体或对等体组，可用 **undo peer** { *ipv4-address* | *group-name* } **advertise-ext-community** 命令恢复缺省配置

说明　表中第 4 步中的 **apply community** 命令有多种应用方式。现假设原 BGP 路由的团体名为 30，在符合路由策略过滤条件的情况下，替换或追加 AS 规则的示例如下。

① 如果配置了 **apply community 100** 命令，则团体名更改为 100。

② 如果配置了 **apply community 100 150** 命令，则团体名更改为 100 或 150，即 BGP 路由属于两个团体。

③ 如果配置了 **apply community 100 150 additive** 命令，则团体名更改为 30、100 或 150，即 BGP 路由属于三个团体。

【示例 1】配置名为 setcommunity 的路由策略，匹配 AS-path-filter 为 8 的路由，更改其团体属性为 no-export。

```
<Huawei> system-view
[Huawei] route-policy setcommunity permit node 16
[Huawei-route-policy] if-match as-path-filter 8
[Huawei-route-policy] apply community no-export
```

【示例 2】将 100:2、1.1.1.1:22、100.100:100 这三个扩展团体属性值添加到 BGP 的 VPN Route-Target 扩展团体属性中

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply extcommunity rt 100:2 rt 1.1.1.1:22 rt 100.100:100 additive
```

14.7.8　配置 BGP 负载分担

在大型网路中，到达同一目的地通常会存在多条有效路由，但是 BGP 只将最优路由发布给对等体，这一特点往往会造成很多流量负载不均衡的情况。通过配置 BGP 负载分担，可以使流量负载均衡，减少网络拥塞。

一般情况下，只有在“BGP 协议的选路规则”中所描述的前 8 个属性完全相同（参见 14.5.1 节），且 AS-Path 属性也相同时，BGP 路由之间才能相互等价，实现 BGP 的负载分担。具体条件如下。

① 原始下一跳（也就是路由到达设备前的下一跳）不相同。

② 首选值（PrefVal）相同。

③ 本地优先级（Local_Pref）相同。

④ 都是聚合路由，或者都不是聚合路由。

⑤ Origin 类型（IGP、EGP、Incomplete）相同。

⑥ MED 值相同。

⑦ 都是 EBGP 路由或都是 IBGP 路由。

⑧ AS 内部 IGP 的 Metric 相同。

⑨ AS_Path 属性完全相同。

但以上路由负载分担的规则也可以通过配置来改变，如忽略路由 AS-Path 属性的比较、忽略 IGP Meric 的比较，但这些配置需要确保不会引起路由环路。

说明 如果实现了 BGP 负载分担，则无论是否配置了 **peer** { *group-name* | *ipv4-address* } **next-hop-local** 命令，在向 IBGP 对等体组发布路由时都先将下一跳地址改变为自身出接口 IP 地址。

BGP 负载分担的配置主要有两个方面：一是配置允许实施负载分担的最大等价路由条数；二是配置在进行负载分担时是否比较 AS_Path 属性。具体的配置步骤如表 14-20 所示。

表 14-20　　BGP 负载分担配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置 BGP 负载分担的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的负载分担配置**
4	**maximum load-balancing** [**ebgp** | **ibgp**] *number* 例如：[Huawei-bgp-af-ipv4] **maximum load-balancing** 2	设置形成负载分担的等价路由的最大条数。命令中的参数和选项说明如下 ● **ebgp**：二选一可选项，指定仅 EBGP 路由形成负载分担，如果同时不指定 ebgp 和 ibgp 选项，则 EBGP 路由和 IBGP 路由之间可以形成负载分担，且形成负载分担的路由条数相同 ● **ibgp**：二选一可选项，指定仅 IBGP 路由形成负载分担 ● *number*：指定形成负载分担的等价路由的最大条数，AR150/160/200 系列、AR1200 系列、AR2201-48FE、AR2202-48FE 和 AR2204 的取值范围为 1～4 的整数，AR2220、AR2220L、AR2240 和 AR3200 系列的取值范围为 1～8 的整数 【注意】本命令新的配置会覆盖旧的配置。在公网中到达同一目的地的路由形成负载分担时，系统会首先判断最优路由的类型。若最优路由为 IBGP 路由则只是 IBGP 路由形成负载分担，若最优路由为 EBGP 路由则只是 EBGP 路由形成负载分担，即**公网中到达同一目的地的 IBGP 路由和 EBGP 路由之间不能形成负载分担**。另外

（续表）

步骤	命令	说明
4	**maximum load-balancing** [**ebgp** | **ibgp**] *number* 例如：[Huawei-bgp-af-ipv4] **maximum load-balancing** 2	● 如果配置了 **maximum load-balancing** *number* 命令，那么再配置 **maximum load-balancing** ebgp *number* 或 **maximum load-balancing** ibgp *number* 命令都不会生效 ● 如果配置了 **maximum load-balancing** ebgp *number* 或 **maximum load-balancing** ibgp *number* 命令，那么再配置 **maximum load-balancing** *number* 命令也不会生效 缺省情况下，形成负载分担的等价路由的最大条数为 1，即不进行负载分担，可用 **undo maximum load-balancing** [**ebgp** | **ibgp**]命令将形成负载分担的指定类型等价路由的最大条数恢复为 1
5	**load-balancing as-path-ignore** 例如：[Huawei-bgp-af-ipv4] **load-balancing as-path-ignore**	（可选）设置路由在形成负载分担时不比较路由的 AS-Path 属性 【说明】该命令主要用于 EBGP 和 IBGP 路由之间进行负载分担的场景，**但在 IPv4 组播网络中，路由在形成负载分担时必须比较 AS-Path 属性，不能配置本命令。**另外，配置路由在形成负载分担时不比较路由的 AS-Path 属性可能会引起路由环路 缺省情况下，路由在形成负载分担时比较路由的 AS-Path 属性，可用 **undo load-balancing as-path-ignore** 命令恢复缺省情况

14.7.9 BGP 路由选路和负载分担管理

配置好以上 BGP 路由选路和负载分担任务，可通过以下 **display** 视图命令查看相关配置，验证配置结果。

① **display bgp paths** [*as-regular-expression*]：查看 BGP 的 AS 路径信息。

② **display bgp routing-table different-origin-as**：查看源 AS 不一致（目的地址相同）的路由。

③ **display bgp routing-table regular-expression** *as-regular-expression*：查看匹配 AS 正则表达式的路由信息。

④ **display bgp routing-table** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]]：查看 BGP 路由表中的信息。

⑤ **display bgp routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**]* [**whole-match**]：查看指定 BGP 团体的路由信息。

⑥ **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }：查看匹配指定 BGP 团体属性过滤器的路由。

⑦ **display bgp multicast routing-table** [*ip-address* [*mask-length* [**longer-prefixes**] | *mask* [**longer-prefixes**]]]：查看 MBGP 路由表的路由信息。

⑧ **display bgp multicast routing-table statistics**：查看 MBGP 路由表的统计信息。

14.7.10 通过 MED 属性控制路由选择的配置示例

本示例的基本拓扑结构如图 14-21 所示，所有路由器都配置 BGP，RouterA 在 AS 65008 中，RouterB 和 RouterC 在 AS 65009 中。RouterA 与 RouterB、RouterC 之间运行 EBGP，RouterB 和 RouterC 之间运行 IBGP。现要求从 AS 65008 到 AS 65009 的流量优先通过 RouterC 到达。

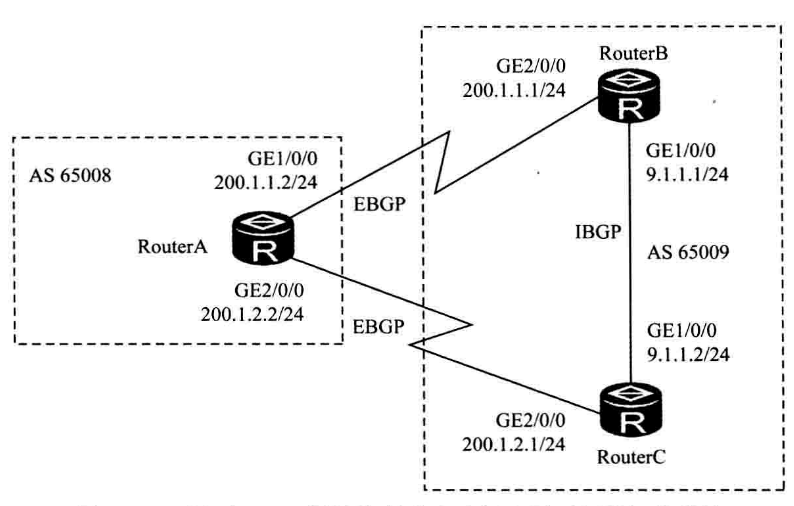


图 14-21　通过 MED 属性控制路由选择配置示例的拓扑结构

1. 基本配置思路分析

本示例的配置比较简单，只需在配置好基本的 BGP 功能，建立各处的 EBGP 或者 IBGP 对等体连接后，再把 RouterB 的 MED 属性调大（而 RouterC 的 MED 属性采用缺省的最小值 0）即可，这样就可以使 RouterA 选择 RouterC 作为流量发往 AS 65009 的入口设备。当然，首先也要为各路由器接口配置好 IP 地址。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 200.1.1.2 24
[RouterA-GigabitEthernet1/0/0]quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 200.1.2.2 24
[RouterA-GigabitEthernet2/0/0]quit
```

② 配置各路由器的 BGP 基本功能。包括配置各自的对等体连接，并需要在 RouterB 和 RouterC 上引入它们之间的直连路由 9.1.1.0/24（主要用于后面的 BGP 路由表验证）。又因本示例没有配置 Loopback 接口，所以需要明确配置各路由器的 Router ID，因为在没有明确配置路由器 ID 的情况下是优先以 Loopback 接口 IP 地址作为路由器 ID 的。为方便记忆，RouterA、RouterB 和 RouterC 的路由器 ID 分别设为 1.1.1.1、2.2.2.2 和 3.3.3.3。

RouterA 上的配置如下。

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.1.1 as-number 65009
[RouterA-bgp] peer 200.1.2.1 as-number 65009
[RouterA-bgp] quit
```

RouterB 上的配置如下。

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.1.2 as-number 65008
[RouterB-bgp] peer 9.1.1.2 as-number 65009
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterB-bgp-af-ipv4] quit
[RouterB-bgp] quit
```

RouterC 上的配置如下。

```
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.2.2 as-number 65008
[RouterC-bgp] peer 9.1.1.1 as-number 65009
[RouterC-bgp] ipv4-family unicast
[RouterC-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterC-bgp-af-ipv4] quit
[RouterC-bgp] quit
```

此时可通过 **display bgp routing-table** 9.1.1.0 24 命令查看 RouterA 的 BGP 路由表中是否有 9.1.1.0/24 这条路由。输出如下，从中可以看出，到目的地址 9.1.1.0/24 有两条有效路由，其中下一跳为 200.1.1.1 的路由是最优路由（因为 RouterB 的 Router ID 要小一些），通告到了 RouterB 和 RouterC（**参见输出信息中的粗体字部分**），来自 RouterC 的非最优路由没有被通告。

```
[RouterA] display bgp routing-table 9.1.1.0 24

 BGP local router ID : 1.1.1.1
 Local AS number : 65008
 Paths:    2 available, 1 best, 1 select
 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.1.1 (2.2.2.2)
 Route Duration: 00h00m56s
 Direct Out-interface: GigabitEthernet1/0/0
 Original nexthop: 200.1.1.1
 Qos information : 0x0
 AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, best, select, pre 255
 Advertised to such 2 peers:
    200.1.1.1
    200.1.2.1

 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (3.3.3.3)
 Route Duration: 00h00m06s
 Direct Out-interface: GigabitEthernet2/0/0
 Original nexthop: 200.1.2.1
 Qos information : 0x0
 AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, pre 255, not preferred for router ID
 Not advertised to any peer yet
```

③ 通过策略配置 RouterB 发送给 RouterA 的 MED 值为 100，使它的优先级降低，而 RouterC 仍采用缺省的最低 MED 值 0（优先级最高）。因为本示例仅需要为发给 EBGP 对等体 RouterA 的路由改变 MED 属性值，所以需要用到路由策略。如果是把 RouterB 上所有 BGP 路由都改变 MED 属性值，则可直接用 **default med** *med* 命令。

```
[RouterB] route-policy policy10 permit node 10
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] bgp 65009
[RouterB-bgp] peer 200.1.1.2 route-policy policy10 export   !---指定将发往对等体 RouterA 的路由 MED 属性值配置为 100
```

此时再可以通过 **display bgp routing-table** 9.1.1.0 24 命令查看 RouterA 的 BGP 路由表中的 9.1.1.0/24 这条路由。从中可以看出，由于下一跳为 200.1.1.1（RouterB）的路由 MED 值为 100，而下一跳为 200.1.2.1 的 MED 值为 0，所以 BGP 优先选择来自 RouterC 的，MED 值较小的路由，并通告到了 RouterB 和 RouterC（**参见输出信息中的粗体字部分**），来自 RouterB 的非最优路由没有被通告。

```
[RouterA] display bgp routing-table 9.1.1.0 24

BGP local router ID : 1.1.1.1
 Local AS number : 65008
 Paths:    2 available, 1 best, 1 select
 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (3.3.3.3)
 Route Duration: 00h07m45s
 Direct Out-interface: GigabitEthernet2/0/0
 Original nexthop: 200.1.2.1
 Qos information : 0x0
 AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, best, select, pre 255
 Advertised to such 2 peers:
    200.1.1.1
    200.1.2.1

 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.1.1 (2.2.2.2)
 Route Duration: 00h00m08s
 Direct Out-interface: GigabitEthernet1/0/0
 Original nexthop: 200.1.1.1
 Qos information : 0x0
 AS-path 65009, origin igp, MED 100, pref-val 0, valid, external, pre 255, not preferred for MED
 Not advertised to any peer yet
```

14.7.11 BGP 团体配置示例

本示例的基本拓扑结构如图 14-22 所示，RouterB 分别与 RouterA、RouterC 之间建立 EBGP 连接。现要求 AS10 发布到 AS20 中的路由不再被 AS20 向其他 AS 发布。

1. 基本配置思路分析

本示例的配置也比较简单，只需要先配置好各路由器的 BGP 基本功能，然后在 RouterA 上利用路由策略定义发往对等体 RouterB 的路由带有 No_Export 团体属性，就可实现 AS10 发布到 AS20 中的路由不再被 AS20 向其他 AS 发布。当然，首先也要为各路由器接口配置好 IP 地址。

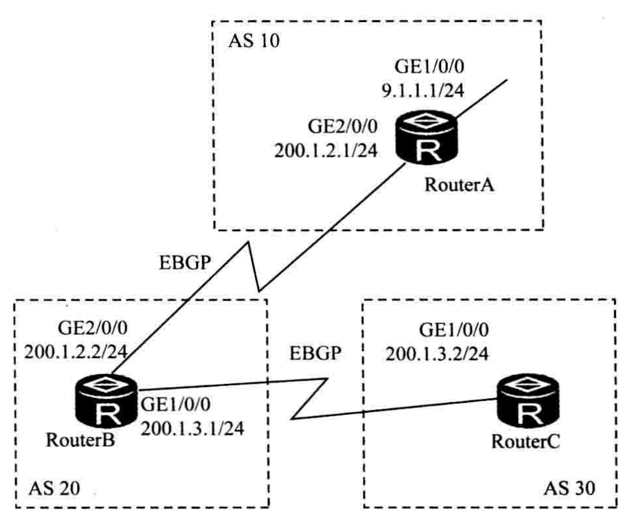


图 14-22　BGP 团体属性配置示例拓扑结构

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 200.1.2.1 24
[RouterA-GigabitEthernet2/0/0]quit
```

② 配置各路由器的 BGP 基本功能。包括配置各自的对等体连接，并需要在 RouterA 上引入它的直连路由 9.1.1.0/24（主要用于后面的 BGP 路由表验证）。又因本示例没有配置 Loopback 接口，所以需要明确配置各路由器的 Router ID。这是因为在没有明确配置路由器 ID 的情况下是优先以 Loopback 接口 IP 地址作为路由器 ID 的。为方便记忆，RouterA、RouterB 和 RouterC 的路由器 ID 分别设为 1.1.1.1、2.2.2.2 和 3.3.3.3。

RouterA 上的配置如下。

```
[RouterA] bgp 10
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.2.2 as-number 20
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterA-bgp-af-ipv4] quit
[RouterA-bgp] quit
```

RouterB 上的配置如下。

```
[RouterB] bgp 20
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.2.1 as-number 10
[RouterB-bgp] peer 200.1.3.2 as-number 30
[RouterB-bgp] quit
```

RouterC 上的配置如下。

```
[RouterC] bgp 30
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.3.1 as-number 20
[RouterC-bgp] quit
```

此时可通过 **display bgp routing-table** 9.1.1.0 命令在 RouterB 上的 BGP 路由表中查看路由 9.1.1.0/24 的详细信息。输出信息如下，从中可以看到 RouterB 把收到的 BGP 路由发布给了位于 AS30 内的 RouterC（**参见输出信息中的粗体字部分**）。

```
[RouterB] display bgp rou ting-table 9.1.1.0
 BGP local router ID : 2.2.2.2
 Local AS number : 20
 Paths:    1 available, 1 best, 1 select
 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (1.1.1.1)
 Route Duration: 00h00m42s
 Direct Out-interface: GigabitEthernet2/0/0
 Original nexthop: 200.1.2.1
 Qos information : 0x0
 AS-path 10, origin igp, MED 0, pref-val 0, valid, external, best, select, active, pre 255
 Advertised to such 2 peers:
    200.1.2.1
    200.1.3.2
```

也可以通过 **display bgp routing-table** 命令查看 RouterC 的 BGP 路由表，从中可以发现 RouterC 已从 RouterB 那里学习到了目的地址为 9.1.1.0/24 的路由（**参见输出信息中的粗体字部分**）。

```
[RouterC] display bgp routing-table
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         200.1.3.1                           0      20 10i
```

③ 在 RouterA 上通过路由策略配置 BGP 团体属性，使 RouterA 发布给 RouterB 的 BGP 路由不再被 RouterB 发布给其他 AS。

```
[RouterA] route-policy comm_policy permit node 10
[RouterA-route-policy] apply community no-export
[RouterA-route-policy] quit
[RouterA] bgp 10
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] peer 200.1.2.2 route-policy comm_policy export
[RouterA-bgp-af-ipv4] peer 200.1.2.2 advertise-community
```

此时再可在 RouterB 上通过 **display bgp routing-table** 9.1.1.0 命令查看 BGP 路由表中的 9.1.1.0/24 的详细信息，从中可以看到 9.1.1.0/24 这条路由携带的团体属性，并且 RouterB 没有把 9.1.1.0/24 这条路由发布给其他区域的对等体（**参见输出信息中的粗体字部分**）。

```
[RouterB] display bgp routing-table 9.1.1.0
 BGP local router ID : 2.2.2.2
 Local AS number : 20
 Paths:    1 available, 1 best, 1 select
 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (1.1.1.1)
```

```
Route Duration: 00h00m09s
Direct Out-interface: GigabitEthernet2/0/0
Original nexthop: 200.1.2.1
Qos information : 0x0
Community:no-export
AS-path 10, origin igp, MED 0, pref-val 0, valid, external, best, select, active, pre 255
Not advertised to any peer yet
```

14.7.12　BGP 负载分担配置示例

本示例的基本拓扑结构如图 14-23 所示，所有路由器都配置 BGP，RouterA 在 AS100 中，RouterB 和 RouterC 在 AS300 中，RouterD 在 AS200 中。现要求充分利用网络资源，减少 RouterA 到目的地址 8.1.1.0/24 网络拥塞。

1. 基本配置思路分析

本示例的配置也比较简单，只需要先配置好各路由器的 BGP 基本功能，然后在 RouterA 上配置负载分担功能，使从 RouterA 发送的流量可以经过 RouterB 和 RouterC 两条路径到达 RouterD，实现对网络资源的充分利用。当然，首先也要为各路由器接口配置好 IP 地址。

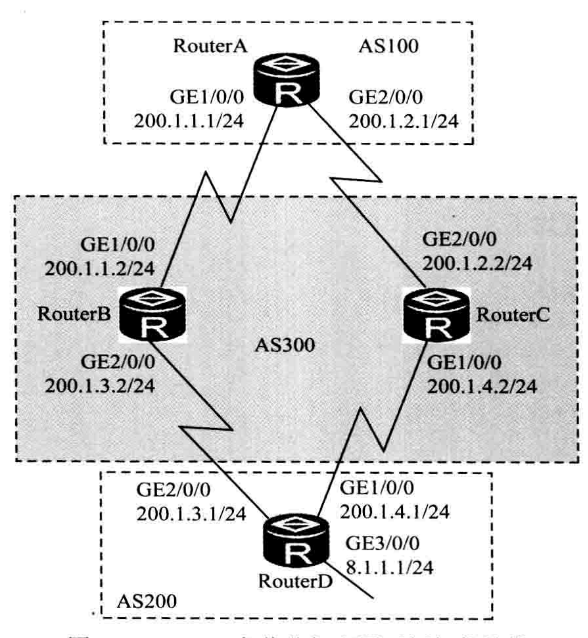


图 14-23　BGP 负载分担配置示例拓扑结构

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 200.1.1.1 24
[RouterA-GigabitEthernet1/0/0]quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 200.1.2.1 24
[RouterA-GigabitEthernet2/0/0]quit
```

② 配置各路由器的 BGP 基本功能。包括配置各自的对等体连接，并需要在 RouterD 上引入它的直连路由 8.1.1.0/24（主要用于后面的 BGP 路由表验证）。又因本示例没有配置 Loopback 接口，所以需要明确配置各路由器的 Router ID。这是因为在没有明确配置路由器 ID 的情况下是优先以 Loopback 接口 IP 地址作为路由器 ID 的。为方便记忆，RouterA、RouterB、RouterC 和 RouterD 的路由器 ID 分别设为 1.1.1.1、2.2.2.2、3.3.3.3 和 4.4.4.4。

RouterA 上的配置如下。

```
[RouterA] bgp 100
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.1.2 as-number 300
[RouterA-bgp] peer 200.1.2.2 as-number 300
[RouterA-bgp] quit
```

RouterB 上的配置如下。

```
[RouterB] bgp 300
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.1.1 as-number 100
[RouterB-bgp] peer 200.1.3.1 as-number 200
[RouterB-bgp] quit
```

RouterC 上的配置如下。

```
[RouterC] bgp 300
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.2.1 as-number 100
[RouterC-bgp] peer 200.1.4.1 as-number 200
[RouterC-bgp] quit
```

RouterD 上的配置如下。

```
[RouterD] bgp 200
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 200.1.3.2 as-number 300
[RouterD-bgp] peer 200.1.4.2 as-number 300
[RouterD-bgp] ipv4-family unicast
[RouterD-bgp-af-ipv4] network 8.1.1.0 255.255.255.0
[RouterD-bgp-af-ipv4] quit
[RouterD-bgp] quit
```

此时可通过 **display bgp routing-table** 8.1.1.0 24 命令查看 RouterA 的 BGP 路由表中目的地址为 8.1.1.0/24 的路由。从路由表中可以看出，RouterA 到目的地址 8.1.1.0/24 有两条有效路由，其中下一跳为 200.1.1.2 的路由是最优路由（因为 RouterB 的 Router ID 要小一些）（**参见输出信息中的粗体字部分**）。

```
[RouterA] display bgp routing-table 8.1.1.0 24

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Paths : 2 available, 1 best, 1 select
 BGP routing table entry information of 8.1.1.0/24:
 From: 200.1.1.2 (2.2.2.2)
 Route Duration: 00h00m50s
 Direct Out-interface: GigabitEthernet1/0/0
 Original nexthop: 200.1.1.2
 Qos information : 0x0
 AS-path 300 200, origin igp, pref-val 0, valid, external, best, select, active, pre 255
```

```
Advertised to such 2 peers:
    200.1.1.2
    200.1.2.2

BGP routing table entry information of 8.1.1.0/24:
From: 200.1.2.2 (3.3.3.3)
Route Duration: 00h00m51s
Direct Out-interface: GigabitEthernet2/0/0
Original nexthop: 200.1.2.2
Qos information : 0x0
AS-path 300 200, origin igp, pref-val 0, valid, external, pre 255, not preferred for router ID
Not advertised to any peer yet
```

③ 在 RouterA 上配置负载分担，允许两条等价路由。

```
[RouterA] bgp 100
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] maximum load-balancing 2
[RouterA-bgp-af-ipv4] quit
[RouterA-bgp] quit
```

此时再通过 **display bgp routing-table** 8.1.1.0 24 命令检查 RouterA 的 BGP 路由表中的 8.1.1.0/24 路由信息。从中可以看到，BGP 路由 8.1.1.0/24 存在两个下一跳，分别是 200.1.1.2 和 200.1.2.2，且都被优选（**参见输出信息中的粗体字部分**）。

```
[RouterA] display bgp routing-table 8.1.1.0 24

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Paths : 2 available, 1 best, 2 select
 BGP routing table entry information of 8.1.1.0/24:
 From: 200.1.1.2 (2.2.2.2)
 Route Duration: 00h03m55s
 Direct Out-interface: GigabitEthernet1/0/0
 Original nexthop: 200.1.1.2
 Qos information : 0x0
 AS-path 300 200, origin igp, pref-val 0, valid, external, best, select,   active, pre 255
 Advertised to such 2 peers
    200.1.1.2
    200.1.2.2

 BGP routing table entry information of 8.1.1.0/24:
 From: 200.1.2.2 (3.3.3.3)
 Route Duration: 00h03m56s
 Direct Out-interface: GigabitEthernet2/0/0
 Original nexthop: 200.1.2.2
 Qos information : 0x0
 AS-path 300 200, origin igp, pref-val 0, valid, external, select,   active, pre 255, not preferred for router ID
 Not advertised to any peer yet
```

14.8 简化 IBGP 网络连接

通过本章前面的学习我们已经知道，BGP 规定，在 AS 内部 IBGP 设备之间，为了防止路由环路，IBGP 设备从其 IBGP 对等体学习来的路由不再通告给其他 IBGP 对等体，

也就是只能单跳通告。这样一来，在 AS 内部各 IBGP 设备之间就可能无法实现互联互通，因为任何一个 IBGP 设备都可能无法了解同一个 AS 中非直连的 IBGP 设备上的路由信息。

为了解决以上问题，会要求 AS 内部的各 IBGP 对等体间全连接，但现实中往往很难做到。为了简化 IBGP 网络连接，BGP 提出了两种解决方案，那就是“路由反射器”和“联盟”，具体参见 14.4 节相关内容。也正因为如此，简化 IBGP 网络连接涉及以下两项配置任务。这两项任务是并列的，可根据实际需要选择其中一个方案，也可同时配置（在配置了联盟后又同时配置路由反射器时，路由反射器是在联盟的子 AS 中进行配置的）。

① 配置 BGP 路由反射器。

② 配置 BGP 联盟。

14.8.1 配置 BGP 路由反射器

在 AS 内部，为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。当 IBGP 对等体数目很多时，建立全连接网络的开销很大。使用路由反射器 RR（Route Reflector），可以解决这个问题。具体的配置步骤如表 14-21 所示（**在需要配置为路由反射器的设置上进行配置**）。在配置前，**要先配置整个网络的 BGP 基本功能，建立 BGP 对等体连接。**

注意 在配置路由反射器时要注意以下几个方面。

① 集群 ID 用于防止集群内多个路由反射器和集群间的路由环路。当一个集群里有多个路由反射器时，必须为同一个集群内的所有路由反射器配置相同的集群 ID。

② 如果路由反射器的客户机之间重新建立了 IBGP 全连接关系，那么客户机之间的路由反射就是没有必要的，而且还占用带宽资源。此时，可以配置禁止客户机之间的路由反射，减轻网络负担。

③ 在一个 AS 内，RR 主要有路由传递和流量转发两个作用。当 RR 连接了很多客户机和非客户机时，同时进行路由传递和流量转发会使 CPU 资源消耗很大，影响路由传递的效率。如果需要保证路由传递的效率，可以在该 RR 上禁止 BGP 将优先的路由下发到 IP 路由表，使 RR 主要用来传递路由。

表 14-21 BGP 路由反射器的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要配置路由反射器的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的路由反射器配置**

（续表）

步骤	命令	说明
4	**peer** { *ipv4-address* | *group-name* } **reflect-client** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **reflect-client**	配置将本机作为路由反射器，并将对等体（组）作为路由反射器的客户。命令中的参数 *ipv4-address* | *group-name* 用来指定要作为路由反射器客户的 IBGP 对等体的 IP 地址或者 IBGP 对等体组 缺省情况下，BGP 未配置路由反射器及其客户，可用 **undo peer** { *group-name* | *ipv4-address* } **reflect-client** 命令删除指定的路由反射器配置
5	**reflector cluster-id** *cluster-id* 例如：[Huawei-bgp-af-ipv4] **lreflector cluster-id** 50	（可选）配置路由反射器的集群 ID，取值范围为 1～4 294 967 295 的整数，也可以用 IP 地址形式标识 【注意】**需要为同一集群内所有的路由反射器配置相同的集群 ID**，以便标识这个集群，避免路由环路。另外，为了保证客户机可以学习到反射器发来的路由，**集群 ID 不能和集群内某客户机的 Router ID 相同**，否则该客户机会将收到的路由丢弃 缺省情况下，每个路由反射器使用自己的 Router ID 作为集群 ID，可用 **undo reflector cluster-id** 命令恢复缺省配置
6	**undo reflect between-clients** 例如：[Huawei-bgp-af-ipv4] **undo reflect between-clients**	（可选）禁止客户机之间的路由反射 缺省情况下，客户机之间的路由反射是允许的，可用 **reflect between-clients** 命令使能客户机之间的路由反射
7	**bgp-rib-only** [**route-policy** *route-policy-name*] 例如：[Huawei-bgp-af-ipv4] **bgp-rib-only**	（可选）禁止 BGP 将优选的路由下发到 IP 路由表。命令中的可选参数 **route-policy** *route-policy-name* 指定用来过滤禁止下发到 IP 路由表中的路由的路由策略 【说明】在反射器场景下，如果 BGP 的优选路由不需要指导转发，通过配置本领，使所有或指定的 BGP 的优选路由不加入 IP 路由表，也不进入转发层，从而提高转发效率和提升系统容量 缺省情况下，BGP 将优选的路由下发到 IP 路由表，可用 **undo bgp-rib-only** 命令恢复缺省配置

14.8.2　配置 BGP 联盟

BGP 联盟是用来解决 AS 内部各 IBGP 设备间必须全连接的另一个方案。它将一个自治系统划分为若干个子自治系统，每个子自治系统内部的 IBGP 对等体建立全连接关系或者配置反射器，子自治系统之间建立 EBGP 连接关系。

在大型 BGP 网络中，配置联盟不但可以减少 IBGP 连接的数量，还可以简化路由策略的管理，提高路由的发布效率。如果其他品牌的路由器的联盟实现机制不同于华为 AR 系列路由器采用的 RFC3065 标准，还可以配置联盟的兼容性，以便和非标准的设备兼容。

BGP 联盟的具体配置步骤如表 14-22 所示。

【经验之谈】因为联盟技术会重新划分子 AS，所以同一 AS 内部的 IBGP 对等体之间的建立是在建立联盟后，是利用新的子 AS 号建立的，不是先利用原来的主 AS 号建立 IBGP 对等体连接，包括联盟内部与外部 AS 之间的 EBGP 对等体的建立，也是用子 AS 号，而不是用原来的主 AS 号。

表 14-22 **BGP 联盟的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**confederation id** { *as-number-plain* | *as-number-dot* } 例如：[Huawei-bgp] **confederation id** 9	配置联盟 ID。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步 缺省情况下，BGP 联盟未配置，可用 **undo confederation id** 命令删除指定的 BGP 联盟
4	**confederation peer-as** { *as-number-plain* | *as-number-dot* } &<1-32> 例如：[Huawei-bgp] **confederation peer-as** 1091 1092 1093	指定与本地设备属于同一个联盟，但**有直接连接**的对端子 AS 号。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步，只不过，这里的 AS 号为聪明的子 AS 号 【说明】命令中定义的子 AS 属于一个联盟内部，每个子 AS 内必须全连接。子 AS 间要通过 **peer** *ipv4-address* **as-number** { *as-number-plain* | *as-number-dot* } 命令彼此建立 EBGP 连接。**没有直接连接的子 AS 的编号不要加入本命令中** 缺省情况下，联盟中未配置子 AS 号，可用 **undo confederation peer-as** { *as-number-plain* | *as-number-dot* } &<1-32>命令删除联盟中指定的子 AS
5	**confederation nonstandard** 例如：[Huawei-bgp] **confederation nonstandard**	（可选）配置联盟中的标准设备（实现机制为 RFC3065）可与非标准设备互通 【注意】在已配置了联盟 ID 的前提下，配置该命令会引起 IBGP 邻居和联盟 EBGP 邻居会话断开连接，再重新建立连接 缺省情况下，联盟中只有标准设备才能互通，可用 **undo confederation nonstandard** 命令配置联盟中只有标准设备才能互通

14.8.3 BGP 路由反射器配置示例

本示例的基本拓扑结构如图 14-24 所示，在一个 AS 中有 8 台设备需要组建 IBGP 网络，其中 RouterB、RouterD 和 RouterE 已经建立了 BGP 全连接。现要求在不破坏 RouterB、RouterD 和 RouterE 全连接关系的情况下采用路由器反射方案组建 IBGP 网络，并尽可能地简化设备的配置和管理。示例中各路由器接口的 IP 地址如表 14-23 所示。

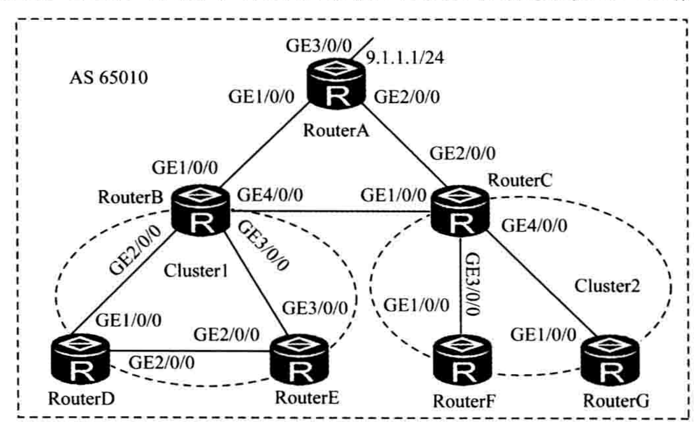


图 14-24 BGP 路由反射器配置示例拓扑结构

表 14-23　　示例中各路由器接口 IP 地址

设备	接口	IP 地址	设备	接口	IP 地址
RouterA	GE 1/0/0	10.1.1.2/24	RouterC	GE 4/0/0	10.1.8.1/24
	GE 2/0/0	10.1.3.2/24	RouterD	GE 1/0/0	10.1.4.2/24
	GE 3/0/0	9.1.1.1/24		GE 2/0/0	10.1.6.1/24
RouterB	GE 1/0/0	10.1.1.1/24	RouterE	GE 2/0/0	10.1.6.2/24
	GE 2/0/0	10.1.4.1/24		GE 3/0/0	10.1.5.2/24
	GE 3/0/0	10.1.5.1/24	RouterF	GE 1/0/0	10.1.7.2/24
	GE 4/0/0	10.1.2.1/24	RouterG	GE 1/0/0	10.1.8.2/24
RouterC	GE 1/0/0	10.1.2.2/24			
	GE 2/0/0	10.1.3.1/24			
	GE 3/0/0	10.1.7.1/24			

1. 基本配置思路分析

本示例除了要在各路由器上配置基本的 BGP 功能外，最重要的配置就是要采用路由器反射技术实现那些非彼此直接连接的 IBGP 设备间的互联。

分析示例中各路由器的连接情况可以发现，RouterA、RouterB 和 RouterC 之间已经分别建立了 BGP 全连接，所以它们之间无需采用路由器反射技术，要禁止客户间的路由反射。另外两部分，RouterB、RouterD 和 RouterE 之间虽然也建立了全连接，但它与 RouterA、RouterB 和 RouterC 之间的全连接有一个共同的设备——RouterB。

另一个部分 RouterC、RouterF 和 RouterG 之间没有建立全连接，但与 RouterA、RouterB 和 RouterC 之间的全连接有一个共同的设备——RouterC，这样一来就可以把 RouterB、RouterD 和 RouterE，以及 RouterC、RouterF 和 RouterG 分别划到一个集群中，通过它们与 RouterA、RouterB 和 RouterC 之间共用的设备作为路由反射器，就可以实现整个 AS 内 IBGP 路由的简单互联，最终实现类似于仅 RouterA、RouterB 和 RouterC 之间全连接的那样的 IBGP 网络。

根据以上分析可以得出本示例的基本配置思路如下。

① 配置 RouterB 是 Cluster1 的路由反射器，RouterD 和 RouterE 是它的两个客户机，配置禁止客户机间通信（**因为它们彼此间已是全连接**），实现在不破坏 RouterB、RouterD 和 RouterE 全连接关系的情况下组建 IBGP 网络的需求。

② 配置 RouterC 为 Cluster2 的路由反射器，RouterF 和 RouterG 是它的客户机，实现简化设备的配置和管理的需求。

当然，在配置路由反射器之前仍然需要先为各路由器接口配置 IP 地址，配置各 IBGP 设备间的基本 BGP 功能，建立 IBGP 对等体连接。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterA-GigabitEthernet1/0/0]quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.3.2 24
```

```
[RouterA-GigabitEthernet2/0/0]quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 9.1.1.1 24
[RouterA-GigabitEthernet3/0/0]quit
```

② 配置各路由器的 BGP 基本功能。包括配置各自的对等体连接，并需要在 RouterD 上引入它的直连路由 8.1.1.0/24（主要用于后面的 BGP 路由表验证）。又因本示例没有配置 Loopback 接口，所以需要明确配置各路由器的 Router ID。这是因为在没有明确配置路由器 ID 的情况下是优先以 Loopback 接口 IP 地址作为路由器 ID 的。为方便记忆，RouterA、RouterB、RouterC、RouterD、RouterE、RouterF、RouterG 的路由器 ID 分别设为 1.1.1.1、2.2.2.2、3.3.3.3、4.4.4.4、5.5.5.5、6.6.6.6 和 7.7.7.7。

具体的配置方法很简单，具体参见 14.7.12 小节介绍的配置方法，只不过这里建立的都是 IBGP 对等立体连接。

③ 在 RouterB 上配置 Cluster1 的路由反射器，集群 ID 号为 1。

```
[RouterB] bgp 65010
[RouterB–bgp] group in_rr internal                          !---创建一个名为 in_rr internal 的对等体组
[RouterB–bgp] peer 10.1.4.2 group in_rr                     !---将 RouterD 作为对等体组 in_rr internal 的成员
[RouterB–bgp] peer 10.1.5.2 group in_rr                     !---将 RouterE 作为对等体组 in_rr internal 的成员
[RouterB–bgp] ipv4-family unicast
[RouterB–bgp-af-ipv4] peer in_rr reflect-client             !---将对等体组 in_rr internal 作为路由反射器的客户
[RouterB–bgp-af-ipv4] undo reflect between-clients          !---禁止客户间直接通信
[RouterB–bgp-af-ipv4] reflector cluster-id 1                !---指定集群 ID 号为 1
[RouterB - bgp-af-ipv4] quit
```

④ 在 RouterC 上配置 Cluster2 的路由反射器，集群 ID 号为 2。

```
[RouterC] bgp 65010
[RouterC-bgp] group in_rr internal
[RouterC-bgp] peer 10.1.7.2 group in_rr
[RouterC-bgp] peer 10.1.8.2 group in_rr
[RouterC-bgp] ipv4-family unicast
[RouterC-bgp-af-ipv4] peer in_rr reflect-client
[RouterC-bgp-af-ipv4] reflector cluster-id 2
[RouterC-bgp-af-ipv4] quit
```

配置好后，可通过 **display bgp routing-table** 9.1.1.0 命令查看 RouterD 上的 BGP 路由表中是否可以见到由 RouterA 连接的 9.1.1.0/24 的路由。从中可以看到，RouterD 从 RouterB 那里学到了 RouterA 通告的路由，而且还可以看到该路由的 Originator 和 Cluster_ID 属性（**参见输出信息中的粗体字部分**）。

```
[RouterD] display bgp routing-table 9.1.1.0
BGP local router ID : 4.4.4.4
 Local AS number : 65010
 Paths:    1 available, 0 best, 0 select
 BGP routing table entry information of 9.1.1.0/24:
 From: 10.1.4.1 (2.2.2.2)
 Route Duration: 00h00m14s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 10.1.1.2
 Qos information : 0x0
 AS-path Nil, origin igp, MED 0, localpref 100, pref-val 0, internal, pre 255
 Originator:   1.1.1.1
 Cluster list: 0.0.0.1
 Not advertised to any peer yet
```

同样，可以在 Cluster1 和 Cluster2 的其他客户的 BGP 路由表中见到 9.1.1.0/24 这条路由，表明以上的路由反射器的配置是正确、成功的。

14.8.4　BGP 联盟配置示例

本示例的基本拓扑结构如图 14-25 所示，AS 200 中有多台 BGP 路由器，其中 RouterA、RouterD 和 RouterE 之间是彼此全连接的，其他路由器之间没有全连接。现需要采用 BGP 联盟方案在 AS 200 内减少 IBGP 的连接数。

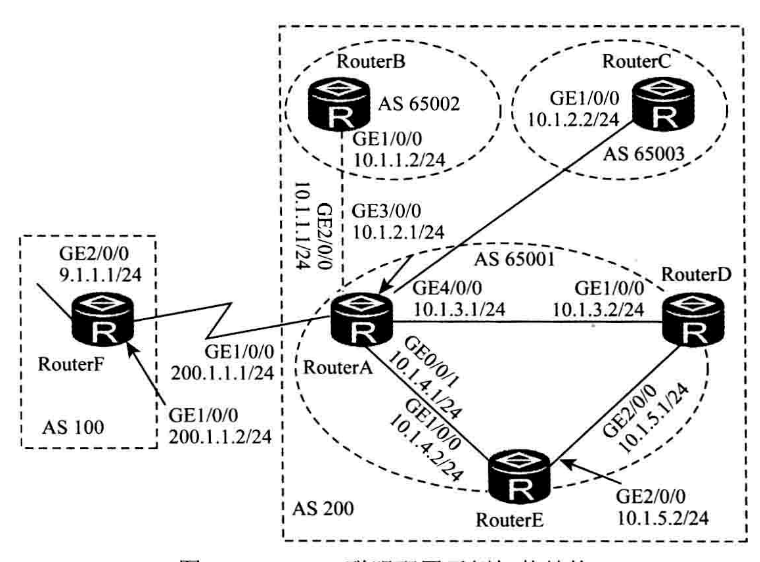


图 14-25　BGP 联盟配置示例拓扑结构

1. 基本配置思路分析

本示例 AS200 内部，RouterA、RouterD 和 RouterE 之间彼此已有全连接，但 RouterB 和 RouterC 没有与其他 IBGP 设备构成全连接。这时可以将整个 AS200 划分为 3 个子 AS：AS 65001、AS 65002 和 AS 65003。其中 RouterA、RouterD 和 RouterE 分到 AS 65001 内，RouterB 和 RouterC 各分别单独分到一个 AS 65002 和 AS 65003 中，可实现减少 IBGP 的连接数的需求。因为 RouterB 和 RouterC 之间没有直接连接，所以不能划分到同一个子 AS 中。

注意　在配置联盟前，仅需配置各路由器的接口 IP 地址，无需配置 BGP 对等体的连接。对等体的连接是在配置好联盟、划分好子 AS 后配置的。

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.1.4.1 24
[RouterA-GigabitEthernet1/0/0]quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0]quit
```

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 10.1.2.1 24
[RouterA-GigabitEthernet3/0/0]quit
[RouterA] interface gigabitethernet 4/0/0
[RouterA-GigabitEthernet4/0/0] ip address 10.1.3.1 24
[RouterA-GigabitEthernet4/0/0]quit
```

② 配置 BGP 联盟。这里其实是要把 RouterA、RouterB 和 RouterC 配置成 EBGP 对等体关系，建立 EBGP 对等体连接。

RouterA 上的配置。这里同时把 RouterB 和 RouterC 所属的子 AS 号加入联盟中，因为 RouterA 与它们都有直接连接。另外，因为 RouterA 是 ASBR 设备，为了使 RouterA 在向它的 IBGP 对等体转发路由时收到路由的 IBGP 对等体可以识别路由中的下一跳，需要在 RouterA 上配置修改转发给 IBGP 对等体的路由的下一跳为自身的出接口 IP 地址。

```
[RouterA] bgp 65001
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] confederation id 200                !---配置联盟 ID 为 200
[RouterA-bgp] confederation peer-as 65002 65003   !---指定与 AS 65001 属于同一个联盟的还有 AS 65002 和 65003
[RouterA-bgp] peer 10.1.1.2 as-number 65002       !---指定 RouterB 为 RouterA 的 EBGP 对等体
[RouterA-bgp] peer 10.1.2.2 as-number 65003
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] peer 10.1.1.2 next-hop-local  !---指定在向 RouterB 进行路由发布时把下一跳设为自己的出接口 IP 地址
[RouterA-bgp-af-ipv4] peer 10.1.2.2 next-hop-local
[RouterA-bgp-af-ipv4] quit
```

RouterB 上的配置。这里不要在 **confederation peer-as** 命令中加入 RouterC 所属的子 AS 号，因为 AS 65002 与 AS 65003 之间没有直接连接。另外，因为 RouterB 不是 ASBR，所以不需要配置修改来自 RouterA 的路由下一跳为自己的出接口。

```
[RouterB] bgp 65002
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] confederation id 200
[RouterB-bgp] confederation peer-as 65001
[RouterB-bgp] peer 10.1.1.1 as-number 65001
[RouterB-bgp] quit
```

RouterC 上的配置。这里也不要在 **confederation peer-as** 命令中加入 RouterB 所属的子 AS 号，也是因为 AS 65003 与 AS 65002 之间没有直接连接。同样因为 RouterC 也不是 ASBR，所以也不要配置修改来自 RouterA 的路由下一跳为自己的出接口。

```
[RouterC] bgp 65003
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] confederation id 200
[RouterC-bgp] confederation peer-as 65001
[RouterC-bgp] peer 10.1.2.1 as-number 65001
[RouterC-bgp] quit
```

③ 配置 AS65001 内的 IBGP 对等体连接。

RouterA 上的配置。这里要注意的是，也要配置把转发给 IBGP 对等体的路由的下一跳修改为自己的出接口 IP 地址。

```
[RouterA] bgp 65001
[RouterA-bgp] peer 10.1.3.2 as-number 65001
[RouterA-bgp] peer 10.1.4.2 as-number 65001
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] peer 10.1.3.2 next-hop-local
[RouterA-bgp-af-ipv4] peer 10.1.4.2 next-hop-local
[RouterA-bgp-af-ipv4] quit
```

RouterD 上的配置如下。

```
[RouterD] bgp 65001
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] confederation id 200
[RouterD-bgp] peer 10.1.3.1 as-number 65001
[RouterD-bgp] peer 10.1.5.2 as-number 65001
[RouterD-bgp] quit
```

RouterE 上的配置如下。

```
[RouterE] bgp 65001
[RouterE-bgp] router-id 5.5.5.5
[RouterE-bgp] confederation id 200
[RouterE-bgp] peer 10.1.4.1 as-number 65001
[RouterE-bgp] peer 10.1.5.1 as-number 65001
[RouterE-bgp] quit
```

④ 配置 AS100 和 AS200 之间的 EBGP 连接。

RouterA 上的配置如下。

```
[RouterA] bgp 65001
[RouterA-bgp] peer 200.1.1.2 as-number 100
[RouterA-bgp] quit
```

RouterF 上的配置如下。

```
[RouterF] bgp 100
[RouterF-bgp] router-id 6.6.6.6
[RouterF-bgp] peer 200.1.1.1 as-number 200
[RouterF-bgp] ipv4-family unicast
[RouterF-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterF-bgp-af-ipv4] quit
```

配置好后，可以通过 **display bgp routing-table** 9.1.1.0 命令查看 RouterB 的 BGP 路由表，从中可以发现 RouterB 已学习到了位于 RouterF 上的 9.1.1.10/24 网络的路由（**参见输出信息中的粗体字部分**）。

```
[RouterB] display bgp routing-table 9.1.1.0
BGP local router ID : 2.2.2.2
 Local AS number : 65002
 Paths:    1 available, 1 best, 1 select
 BGP routing table entry information of 9.1.1.0/24:
 From: 10.1.1.1 (1.1.1.1)
 Route Duration: 00h12m29s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface: GigabitEthernet1/0/0
 Original nexthop: 10.1.1.1
 Qos information : 0x0
 AS-path (65001) 100, origin igp, MED 0, localpref 100, pref-val 0, valid, external-confed, best, select, pre 255
 Not advertised to any peer yet
```

在联盟中的其他 IBGP 设备的 BGP 路由表中同样可以查看到以上 9.1.1.0/24 路由，证明联盟配置成功。

14.9 控制 BGP 路由的发布和接收

控制 BGP 路由的发布和接收，可以控制路由表的容量，提高网络的安全性。控制

BGP 路由的发布和接收是通过路由策略来实现的，但配置路由策略后还需要对 BGP 进行软复位，以便最终应用所配置的路由策略。

另外，BGP 路由聚合也可在一定程度上控制路由的发布和接收，本节将一并进行介绍。路由策略的配置将在下章详细介绍，在此不再赘述。在配置控制 BGP 路由的发布和接收之前，也需配置 BGP 的基本功能。

14.9.1 控制 BGP 路由发布

BGP 路由表路由数量通常比较大，传递大量的路由对设备来说是一个很大的负担。为了减小路由发送规模，需要对发布的路由进行控制，只发送自己想要发布的路由或者只发布对等体需要的路由。另外，到达同一个目的地址，可能存在多条路由，这些路由分别需要穿越不同的 AS，为了把业务流量引导向某些特定的 AS，也需要对发布的路由进行筛选。

根据所控制的范围不同，BGP 路由发布控制有两种方式：一是基于全局对 BGP 设备向所有对等体（组）发布的路由进行控制，二是基于特定对等体（组）发布的路由控制。如果同时配置，则基于特定对等体（组）的配置优先。这两种控制方法的具体配置步骤如表 14-24 所示。

表 14-24　　控制 BGP 路由发布的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要控制 BGP 路由发布的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的路由发布控制配置**
方式一：基本全局的路由发布控制配置		
4	**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] 例如：[Huawei-bgp-af-ipv4] **filter-policy** 2001 **export ospf** 10	配置对发布的路由进行过滤，只有通过过滤的路由才被 BGP 发布。命令中的参数说明如下 ● *acl-number*：多选一参数，指定用于过滤发布的路由的基本 ACL 编号，取值范围为 2 000～2 999 ● **acl-name** *acl-name*：多选一参数，指定用于过滤发布的路由的 ACL 名称，1～32 个字符，不支持空格，区分大小写。且必须以英文字母 a～z 或 A～Z 开始，可以是英文字母、数字、连字符“-”或下划线“_”的组合。但只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则有效 ● **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤发布的路由的 IP 地址前缀列表名称，1～169 个字符，区分大小写，不支持空格 ● *protocol*：可选参数，指定要过滤的路由协议类型，支持 **direct**、**isis**、**ospf**、**rip**、**static**、**unr** ● *process-id*：可选参数，指定当 *protocol* 参数选择为 **isis**、**ospf**、**rip** 时，路由对应的进程号，取值范围为 1～65 535 的整数

（续表）

步骤	命令	说明
4	**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] 例如：[Huawei-bgp-af-ipv4] **filter-policy** 2001 **export ospf** 10	【注意】如果使用 ACL 过滤策略，且 ACL 过滤规则中没有指定某个 VPN 实例，则 BGP 是对所有地址族下的路由信息进行过滤，包括来自公网和私网的路由信息。如果 ACL 过滤规则中指定了 VPN 实例，**则是仅对来自该 VPN 的数据流量进行过滤，而不是对路由信息进行过滤** 缺省情况下，发布的路由信息不被过滤，可用 **undo filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix***ip-prefix-name* } **export** [*protocol* [*process-id*]]命令删除发布路由时应用指定的过滤策略
方式二：基于特定对等体（组）的路由发布控制配置		
4	**peer** { *group-name* | *ipv4-address*} **filter-policy** { *acl-number* | **acl-name** *acl-name* } **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **filter-policy** 2000 **export**	（四选一）配置基于 ACL 向指定对等体（组）发布路由时的过滤策略。命令中的参数说明如下 ● *group-name* | *ipv4-address*：指定要对等体组名称或对等体 IP 地址 ● *acl-number*：多选一参数，指定用于过滤发布的路由的基本 ACL 编号，取值范围为 2 000～2 999 ● **acl-name** *acl-name*：多选一参数，指定用于过滤发布的路由的 ACL 名称，1～32 个字符，不支持空格，区分大小写。且必须以英文字母 a～z 或 A～Z 开始，可以是英文字母、数字、连字符“-”或下划线“_”的组合。但只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则有效 【注意】该命令为覆盖型的命令，即新的配置将覆盖原来的配置 缺省情况下，向对等体（组）发布路由时未配置过滤策略，可用 **undo peer** { *group-name* | *ipv4-address*} **filter-policy** { *acl-number* | **acl-name** *acl-name* } **export** 命令删除向对等体（组）发布路由时应用指定的过滤策略
	peer { *ipv4-address* | *group-name* } **ip-prefix** *ip-prefix-name* **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **ip-prefix list1 export**	（四选一）配置基于 IP 地址前缀列表向指定对等体（组）发布路由时应用的过滤策略。命令中的 *ip-prefix-name* 指定用来过滤发布路由的 IP 地址前缀名称，1～169 个字符，区分大小写，不支持空格。*ipv4-address* | *group-name* 参数说明参见前面介绍的基于 ACL 过滤方式配置说明 缺省情况下，向对等体（组）发布路由时未配置过滤策略，可用 **undo peer** { *ipv4-address* | *group-name* } **ip-prefix** *ip-prefix-name* **export** 命令删除向对等体（组）发布路由时应用指定的 IP 地址前缀列表
	peer { *ipv4-address* | *group-name* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **as-path-filter** 3 **export**	（四选一）配置基于 AS 路径过滤器向指定对等体（组）发布路由时应用的过滤策略。命令中的 *as-path-filter-number* | *as-path-filter-name* 指定过滤发布路由的 AS 路径过滤器编号（取值范围为 1～256 的整数）或 AS 路径过滤器名称（1～51 个字符，区分大小写，**不能是全数字**）。*ipv4-address* | *group-name* 参数说明参见前面介绍的基于 ACL 过滤方式配置说明 【注意】对于相同的对等体地址，只能使用一个 AS 路径过滤器对发布的路由进行过滤

（续表）

步骤	命令	说明
4	**peer** { *ipv4-address* | *group-name* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **as-path-filter** 3 **export**	缺省情况下，向对等体（组）发布路由时未配置过滤策略，可用 **undo peer** { *ipv4-address* | *group-name* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } **export** 命令删除向对等体（组）发布路由时应用指定的 AS 路径过滤器
	peer { *ipv4-address* | *group-name*} **route-policy** *route-policy-name* **export** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **export**	（四选一）配置基于路由策略向指定对等体（组）发布路由时应用的过滤策略。命令中的 *route-policy-name* 指定用来过滤发布路由的路由策略名称，1～40 个字符，区分大小写，不支持空格。*ipv4-address* | *group-name* 参数说明参见前面介绍的基于 ACL 过滤方式配置说明 缺省情况下，向对等体（组）发布路由时未配置过滤策略，可用 **undo peer** { *ipv4-address* | *group-name*} **route-policy** *route-policy-name* **export** 命令删除向对等体（组）发布路由时应用指定的路由策略

14.9.2 控制 BGP 路由信息的接收

当设备遭到恶意攻击或者网络中出现错误配置时，会导致 BGP 从邻居接收到大量的路由，从而消耗大量的设备资源，因此管理员必须根据网络规划和设备容量，对运行时所使用的资源进行限制。BGP 提供了基于对等体（组）的路由控制，限定邻居发来的路由数量。

与路由发布控制一样，接收路由控制也有两种配置方式：一是基于全局的对所有接收的路由进行控制，二是基于来自特定的对等体（组）的路由进行控制。如果同时配置，基于特定对等体（组）的配置优先于基于全局的配置。这两种控制方式的具体配置步骤如表 14-25 所示。

表 14-25　　控制 BGP 路由发布的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	进入要控制 BGP 路由接收的对应 IP 地址族视图。**BGP 路由在不同的地址族视图下可分别配置不同的路由接收控制配置。**
方式一：基本全局的路由接收控制配置		
4	**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import** 例如：[Huawei-bgp-af-ipv4] **filter-policy** 2001 **import**	配置对接收的路由进行过滤，只有通过过滤的路由才被 BGP 接收。命令中的参数说明如下 • *acl-number*：多选一参数，指定用于过滤接收的路由的基本 ACL 编号，取值范围为 2 000～2 999 • **acl-name** *acl-name*：多选一参数，指定用于过滤接收的路由的 ACL 名称，1～32 个字符，不支持空格，区分大小写。且必须以英文字母 a～z 或 A～Z 开始，可以是英文字母、数字、连字符“-”或下划线“_”的组合。但只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则有效

（续表）

步骤	命令	说明
4	**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import** 例如：[Huawei-bgp-af-ipv4] **filter-policy** 2001 **import**	• **ip-prefix** *ip-prefix-name*：多选一参数，指定用于过滤接收的路由的 IP 地址前缀列表名称，1～169 个字符，区分大小写，不支持空格 缺省情况下，接收的路由信息不被过滤，可用 **undo filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix***ip-prefix-name* } **import** 命令删除接收路由时应用指定的过滤策略
方式二：基于特定对等体（组）的路由接收控制配置		
4	**peer** { *group-name* | *ipv4-address*} **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **filter-policy** 2000 **import**	（四选一）配置基于 ACL 从指定对等体（组）接收路由时的过滤策略。命令中的参数说明如下 • *group-name* | *ipv4-address*：指定对等体组名称或对等体 IP 地址 • *acl-number*：多选一参数，指定用于过滤接收的路由的基本 ACL 编号，取值范围为 2 000～2 999 • **acl-name** *acl-name*：多选一参数，指定用于过滤接收的路由的 ACL 名称，1～32 个字符，不支持空格，区分大小写。且必须以英文字母 a～z 或 A～Z 开始，可以是英文字母、数字、连字符“-”或下划线“_”的组合。但只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则有效 【注意】该命令为覆盖型的命令，即新的配置将覆盖原来的配置 缺省情况下，从对等体（组）接收路由时未配置过滤策略，可用 **undo peer** { *group-name* | *ipv4-address*} **filter-policy** { *acl-number* | **acl-name** *acl-name* } **export** 命令删除从对等体(组)接收路由时应用指定的过滤策略
	peer { *ipv4-address* | *group-name* } **ip-prefix** *ip-prefix-name* **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **ip-prefix list1 import**	（四选一）配置基于 IP 地址前缀列表对从指定对等体（组）接收路由时应用的过滤策略。命令中的 *ip-prefix-name* 指定用来过滤接收路由的 IP 地址前缀名称，1～169 个字符，区分大小写，不支持空格。*ipv4-address* | *group-name* 参数说明参见前面介绍的基于 ACL 过滤方式配置说明 缺省情况下，从对等体（组）接收路由时未配置过滤策略，可用 **undo peer** { *ipv4-address* | *group-name* } **ip-prefix** *ip-prefix-name* **export** 命令删除从对等体（组）接收路由时应用指定的 IP 地址前缀列表
	peer { *ipv4-address* | *group-name* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **as-path-filter** 3 **import**	（四选一）配置基于 AS 路径过滤器对从指定对等体（组）接收路由时应用的过滤策略。命令中的 *as-path-filter-number* | *as-path-filter-name* 指定用来过滤接收路由的 AS 路径过滤器编号（取值范围为 1～256 的整数）或 AS 路径过滤器名称（1～51 个字符，区分大小写，**不能是全数字**）。*ipv4-address* | *group-name* 参数说明参见前面介绍的基于 ACL 过滤方式配置说明 【注意】对于相同的对等体地址，只能使用一个 AS 路径过滤器对发布的路由进行过滤 缺省情况下，从对等体（组）接收路由时未配置过滤策略，可用 **undo peer** { *ipv4-address* | *group-name* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } **export** 命令删除从对等体（组）接收路由时应用指定的 AS 路径过滤器

（续表）

步骤	命令	说明
4	**peer** { *ipv4-address* | *group-name*} **route-policy** *route-policy-name* **import** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-policy** test-policy **import**	（四选一）配置基于路由策略对从指定对等体（组）发布路由时应用的过滤策略。命令中的 *route-policy-name* 指定用来过滤接收路由的路由策略名称，1～40 个字符，区分大小写，不支持空格。*ipv4-address* | *group-name* 参数说明参见前面介绍的基于 ACL 过滤方式配置说明 缺省情况下，从对等体（组）接收路由时未配置过滤策略，可用 **undo peer** { *ipv4-address* | *group-name*} **route-policy** *route-policy-name* **export** 命令删除从对等体（组）接收路由时应用指定的路由策略
5	**peer** { *group-name* | *ipv4-address* } **route-limit** *limit* [*percentage*] [**alert-only** | **idle-forever** | **idle-timeout** *times*] 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **route-limit** 5000	（可选）设置允许从对等体收到的路由数量。命令中的参数和选项说明如下 ● *g group-name* | *ipv4-address*：指定对等体组名称或对等体 IP 地址 ● *limit*：指定允许从对等体接收的最大路由数量，AR150 系列的取值范围为 1～1 000 的整数，AR160 系列的取值范围为 1～20 000 的整数，AR200 系列的取值范围为 1～5 000 的整数，AR1200 系列、AR2201-48FE、AR2202-48FE 和 AR2204 的取值范围为 1～30 000 的整数，AR2220 和 AR2220L 的取值范围为 1～80 000 的整数，AR2240 的取值范围为 1～200 000，AR3200 系列的取值范围为 1～500 000 的整数 ● *percentage*：可选参数，指定路由器开始生成告警消息时从指定对待体（组）接收的路由数量所占设置的允许最大路由数量的百分比，取值范围为 1～100 的整数，缺省值为 75，代表 75% ● **alert-only**：多选一可选项，指定在从指定对等体（组）接收的路由数量超出允许的最大路由数量时仅产生告警，并不再接收超限后的路由 ● **idle-forever**：多选一可选项，指定在从指定对等体（组）接收的路由数量超出允许的最大路由数量时断开连接，并不自动重新建立连接，直到执行 **reset bgp** 命令重新建立连接 ● **idle-timeout** *times*：多选一可选项，指定在从指定对等体（组）接收的路由数量超出允许的最大路由数量时断开连接，并设置自动重新建立连接的超时定时器，取值范围为 1～1 200 的整数分钟。在定时器超时前，可执行 **reset bgp** 命令重新建立连接 【说明】如果同时不选择 **alert-only**、**idle-forever**、**idle-timeout** 可选项，则在路由超限产生告警并记入日志，并与对应对等体（组）断开连接，30 s 后自动重新尝试建立对等体关系 缺省情况下，从对等体接收路由没有数量限制，可用 **undo peer** { *group-name* | *ipv4-address* } **route-limit** 命令对从指定对等体（组）接收的路由不做限制

14.9.3 配置 BGP 软复位

在 BGP 设备上按照前面两节介绍的方法配置了发布路由、接收路由策略后，为了使策略立即生效，可以通过 **reset bgp** [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** }

[**graceful**]命令复位指定的 BGP 连接，但这样会造成短暂的 BGP 连接中断。

BGP 支持手动对 BGP 连接进行软复位，即可在不中断 BGP 连接情况下完成路由表的刷新（Route-refresh）。对不支持 Route-refresh 能力的 BGP 对等体，还可同时配置保留该对等体的所有原始路由功能，这样便能在不复位 BGP 连接的情况下完成路由表的刷新。具体配置方法如表 14-26 所示。

表 14-26　对 BGP 连接进行软复位的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	（可选）进入要配置保存原始 BGP 路由的对应 IP 地址族视图，**仅当要软复位的对等体（组）不支持 Route-refresh 功能时才需要配置本步骤**
4	**peer** {*ipv4-address* | *group-name* } **keep-all-routes** 例如：[Huawei-bgp-af-ipv4] **peer** 1.1.1.2 **keep-all-routes**	（可选）保存自 BGP 连接建立起来之后的所有来自指定对等体（组）的 BGP 路由更新信息。**仅当要进行软复位的对等体或对等不支持 Route-refresh 功能时才需要配置本步骤**。如果路由器支持 Route-refresh 功能，不需要配置本命令，否则执行下面的第 8 步 refresh bgp 命令将不生效。命令中的参数 *ipv4-address* |*group-name* 用来指定要保存 BGP 所有原始路由的对等体 IP 地址或对等体组名称 缺省情况下，只保存来自对等体的通过已配置入口策略的 BGP 路由更新信息，可用 **undo peer** { *ipv4-address* | *group-name* } **keep-all-routes** 命令恢复缺省配置
5	**quit** 例如：[Huawei-bgp-af-ipv4] **quit**	退出地址族视图，返回 BGP 视图
6	**peer** { *ipv4-address* | *group-name* } **capability-advertise route-refresh** 例如：[Huawei-bgp] **peer** 160.89.2.33 **capability-advertise route-refresh**	（可选）使能 Route-refresh（路由刷新）能力，**仅当要软复位的对等体（组）支持 Route-refresh 功能时才需要配置本步骤**。命令中的参数 *ipv4-address* | *group-name* 用来指定要进行 BGP 路由刷新的对等体 IP 地址或对等体组名称 缺省情况下，已使能 BGP 路由刷新功能，可用 **undo peer** { *ipv4-address* | *group-name* } **capability-advertise route-refresh** 命令取消对指定对等体（组）进行路由刷新
7	**return** 例如：[Huawei-bgp] **return**	退出 BGP 视图，直接返回用户视图
8	**refresh bgp** [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** } 例如：<Huawei> **refresh bgp all import**	手工对指定 BGP 连接软复位。命令中的参数和选项说明如下 ● **vpn-instance** *vpn-instance-name* **ipv4-family**：二选一可选参数，软复位指定使能了 IP 地址族的 VPN 实例的 BGP 连接 ● **vpnv4**：二选一可选项，软复位与 VPNv4 的相关 BGP 连接，但 AR150/160/200 系列不支持本选项 ● **all**：多选一选项，软复位与[**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**]可选参数中指定的所有 BGP 的 IPv4 连接 ● *ipv4-address* | **group** *group-name*：多选一参数，软复位与 [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] 可选参数中指定的对等体对等组的 BGP 连接

（续表）

步骤	命令	说明
8	**refresh bgp** [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** } 例如：<Huawei> **refresh bgp all import**	• **external**：多选一选项，软复位与[**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**]可选参数中指定的 EBGP 连接 • **internal**：多选一选项，软复位与[**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**]可选参数中指定的 IBGP 连接 • **export**：二选一选项，指定触发符合条件的出方向的软复位 • **import**：二选一选项，指定触发符合条件的入方向的软复位

14.9.4 配置 BGP 路由聚合

IPv4 网络中 BGP 支持自动聚合和手动聚合两种聚合方式，**自动聚合方式只能聚合到对应的自然网段路由**，而手动聚合方式则可以是任何子网掩码长度（**但必须大于 8**）小于被聚合路由子网掩码长度的子网或超网路由。手动聚合仅对 BGP 本地路由表中已经存在的路由表项有效。同时配置时，**自动聚合的路由优先级低于手动聚合的路由优先级。**

BGP 自动路由聚合和手动路由聚合的配置方法如表 14-27 所示。

表 14-27　　BGP 路由聚合的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**ipv4-family** { **unicast** | **multicast** } 例如：[Huawei-bgp] **ipv4-family unicast**	（可选）进入要 BGP 路由聚合的对应 IP 地址族视图
方式 1：配置自动路由聚合		
4	**summary automatic** 例如：[Huawei-bgp-af-ipv4] **summary automatic**	使能对本地引入的路由进行自动聚合功能。引入的路由可以是直连路由、静态路由、RIP 路由、OSPF 路由、IS-IS 路由。但该命令对**network**命令引入的路由无效 配置该命令后，BGP 将按照自然网段聚合路由（如 10.1.1.0/24 和 10.2.1.0/24 将聚合为 A 类地址 10.0.0.0/8），并且 BGP 只向对等体发送聚合后的路由。这样可以减少路由信息的数量 缺省情况下，对本地引入的路由进行自动聚合功能未使能，可用 **undo summary automatic** 命令去使能对本地引入的路由进行自动聚合功能
方式 2：配置手动路由聚合，它们是并列关系，可根据实际需要选择其中一项或多项进行配置		
5	**aggregate** *ipv4-address* { *mask* | *mask-length* } 例如：[Huawei-bgp-af-ipv4] **aggregate** 168.32.0.0 255.255.0.0	（可选）在 BGP 路由表中创建一条聚合路由，但此时**将同时发布所有聚合路由和被聚合的路由**。命令中的参数说明如下 • *ipv4-address*：指定聚合路由的网络 IP 地址 • *mask* | *mask-length*：指定聚合路由的网络 IP 地址所对应的子网掩码（选择二选一参数 *mask* 时）或子网掩码长度（选择二选一参数 *mask-length* 时） 缺省情况下，BGP 路由表中没有创建聚合路由，可用 **undo aggregate** *ipv4-address* { *mask* | *mask-length* }命令在 BGP 路由表中删除指定的聚合路由

（续表）

步骤	命令	说明
6	**aggregate** *ipv4-address* { *mask* | *mask-length* } **detail-suppressed** 例如：[Huawei-bgp-af-ipv4] **aggregate** 168.32.0.0 255.255.0.0 **detail-suppressed**	（可选）在 BGP 路由表中创建一条聚合路由，但此时**将只发布聚合路由**。命令中的参数参见本表前面第 5 步说明 缺省情况下，BGP 路由表中没有创建聚合路由，可用 **undo aggregate** *ipv4-address* { *mask* | *mask-length* } **detail-suppressed** 命令在 BGP 路由表中删除指定的聚合路由
7	**aggregate** *ipv4-address* { *mask* | *mask-length* } **suppress-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **aggregate** 168.32.0.0 255.255.0.0 **suppress-policy** test-policy	（可选）在 BGP 路由表中创建一条聚合路由，但此时**只发布聚合路由和通过路由策略的被聚合的路由**。命令中的参数 *route-policy-name* 用来过滤允许发布的被聚合路由的路由策略，其他参数参见本表前面第 5 步说明 缺省情况下，BGP 路由表中没有创建聚合路由，可用 **undo aggregate** *ipv4-address* { *mask* | *mask-length* } **suppress-policy** *route-policy-name* 命令在 BGP 路由表中删除指定的聚合路由
8	**aggregate** *ipv4-address* { *mask* | *mask-length* } **as-set** 例如：[Huawei-bgp-af-ipv4] **aggregate** 168.32.0.0 255.255.0.0 **as-set**	（可选）在 BGP 路由表中创建具有 AS-SET 的聚合路由，用于检测环路。命令中的参数参见本表前面第 5 步说明 缺省情况下，BGP 路由表中没有创建聚合路由，可用 **undo aggregate** *ipv4-address* { *mask* | *mask-length* } **as-set** 命令在 BGP 路由表中删除指定的聚合路由
9	**aggregate** *ipv4-address* { *mask* | *mask-length* } **attribute-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **aggregate** 168.32.0.0 255.255.0.0 **attribute-policy** test-policy	（可选）在 BGP 路由表中创建一条聚合路由，并且可通过 *route-policy-name* 参数指定的路由策略配置聚合路由属性，其他参数参见本表前面第 5 步说明 缺省情况下，BGP 路由表中没有创建聚合路由，可用 **undo aggregate** *ipv4-address* { *mask* | *mask-length* } **attribute-policy** *route-policy-name* 命令在 BGP 路由表中删除指定的聚合路由
10	**aggregate** *ipv4-address* { *mask* | *mask-length* } **origin-policy** *route-policy-name* 例如：[Huawei-bgp-af-ipv4] **aggregate** 168.32.0.0 255.255.0.0 **origin-policy** test-policy	（可选）在 BGP 路由表中创建一条聚合路由，但只将通过 *route-policy-name* 参数指定的路由策略的路由生成聚合路由，其他参数参见本表前面第 5 步说明 缺省情况下，BGP 路由表中没有创建聚合路由，可用 **undo aggregate** *ipv4-address* { *mask* | *mask-length* } **origin-policy** *route-policy-name* 命令在 BGP 路由表中删除指定的聚合路由

14.10 调整 BGP 网络的收敛速度

通过配置 BGP 定时器、去使能 EBGP 连接快速复位和路由振荡抑制可以提高 BGP 网络的收敛速度，提高 BGP 的稳定性。主要可配置的任务如下。这些任务是并列关系，可根据实际需要选择其中一项或多项进行配置。在配置这些任务之前均需要配置 BGP 的基本功能。

① 配置 BGP 连接重传定时器。

② 配置 BGP 存活时间和保持时间定时器。

③ 配置 BGP 更新报文定时器。

④ 配置 EBGP 连接快速复位。

14.10.1 配置 BGP 连接重传定时器

BGP 发起 TCP 连接后，如果成功建立起 TCP 连接，则关闭连接重传定时器。如果 TCP 连接建立不成功，则会在连接重传定时器超时后重新尝试建立连接。通过设置较小的连接重传定时器，可以减少等待下次连接建立的时间，加快连接失败后重新建立的速度。而设置较大的连接重传定时器，可以减小由于邻居反复振荡引起的路由振荡。

BGP 支持在全局或者单个对等体（组）配置连接重传定时器，具体的配置步骤如表 14-28 所示。如果同时配置，则定时器生效的优先级为单个对等体高于对等体组，对等体组高于全局。

表 14-28　　BGP 连接重传定时器的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**timer connect-retry** *connect-retry-time* 例如：[Huawei-bgp] **timer connect-retry** 60	配置全局 TCP 连接重传定时器。参数 *connect-retry-time* 用来指定 TCP 连接重传时间间隔，取值范围为 1～65 535 的整数秒 缺省情况下，连接重传时间间隔是 32 s，可用 **undo timer connect-retry** 命令恢复全局 TCP 连接重传时间间隔为缺省值
4	**peer** { *group-name* | *ipv4-address* } **timer connect-retry** *connect-retry-time* 例如：[Huawei-bgp] **peer** 1.1.1.2 **timer connect-retry** 60	（可选）配置与指定对等体或对等体组的 TCP 连接重传定时器。命令中的参数 *group-name* | *ipv4-address* 分别用来指定要设置 TCP 连接重传定时器的对等体或对等体组，命令中的 *connect-retry-time* 参数说明参见本表第 3 步 缺省情况下，连接重传时间间隔是 32 s，可用 **undo peer** { *group-name* | *ipv4-address* } **timer connect-retry** 命令恢复与指定对等体或者对等体组的 TCP 连接重传时间间隔为缺省值

14.10.2 配置 BGP 存活时间和保持时间定时器

BGP 的 Keepalive 消息用于维持 BGP 连接关系。减小存活时间和保持时间，BGP 可以更快速地检测到链路的故障，有利于 BGP 网络快速收敛。但是过短的保持时间会导致网络中的 Keepalive 消息增多，使得设备的负担加重，并且会占用一定的网络带宽。

增大存活时间和保持时间，可以减轻设备负担并减少网络带宽的占用。但是过长的保持时间会导致网络中的 Keepalive 消息减少，使得 BGP 不能及时检测到链路状态的变化，不利于 BGP 网络快速收敛，还可能会造成流量损失。

BGP 支持在全局或者单个对等体（组）配置存活时间和保持时间定时器，具体的配置步骤如表 14-29 所示。如果同时配置，则定时器生效的优先级单个对等体高于对等体组，对等体组高于全局。

注意 改变定时器的值会导致路由器之间的 BGP Peer 关系中断。另外，配置的保持时间需要大于 20 s，否则，可能会造成邻居会话的中断。

表 14-29　BGP 存活时间和保持时间定时器的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*] 例如：[Huawei-bgp] **timer keepalive** 30 **hold** 90	配置全局的 keepalive 消息发送间隔和保持时间。命令中的参数说明如下。 ● *keepalive-time*：指定 Keepalive 消息的存活时间间隔，即发送 keepalive 消息的时间间隔，取值范围为 1～21 845 的整数秒 ● *hold-time*：指定 Keepalive 消息的保存时间间隔，取值范围为 0 或 3～65 535 的整数秒，至少要等于 3 倍 *keepalive-time* 参数取值。超过这个时间还没收到新的 Keepalive 消息，则认为对方设备无效 ● *min-holdtime*：可选参数，指定本端可以接受的最小保持时间间隔，取值范围为 20～65 535 的整数秒，但必须大于 *hold-time* 参数取值 【注意】实际的 *keepalive-time* 值和 *hold-time* 值是通过双方协商来确定的。其中，取对等体双方的 Open 报文中的 *hold-time* 的较小值为最终的 *hold-time* 值；取协商的 *hold-time* 值÷3，和本地配置的 *keepalive-time* 值中较小的作为最终的 *keepalive-time* 值。 如果仅仅改变 *min-holdtime* 值，而两端协商的 *keepalive-time* 值和 *hold-time* 值没有改变，则本端并不会中断已经建立的对等体关系。只有当两端再次建立对等体关系时才会将本端配置的 *min-holdtime* 值与对端发过来的 *hold-time* 值相比较，如果本端配置的 *min-holdtime* 值大于对端发过来的 *hold-time* 值，则 *hold-time* 值协商不成功，两端不能建立对等体关系 当 *keepalive-time* 值和 *hold-time* 值同时取 0 时，将导致 BGP 定时器无效，即 BGP 不会根据定时器检测链路故障 缺省情况下，keepalive 消息的存活时间为 60 s，保持时间为 180 s，可用 **undo timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]或者 **undo timer keepalive hold** [**min-holdtime**]命令恢复 keepalive 消息的存活时间与保持时间间隔为缺省值
4	**peer** { *ipv4-address* | *group-name* } **timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*] 例如：[Huawei-bgp] **peer** 1.1.1.2 **timer keepalive** 10 **hold** 30	（可选）配置对等体或对等体组的 keepalive 消息发送间隔和保持时间。命令中的参数 *ipv4-address* | *group-name* 分别用来指定要设置 keepalive 发送间隔和保持时间的对等体或对等体组，其他参数及注意事项说明参见本表第 3 步 缺省情况下，keepalive 消息的存活时间为 60 s，保持时间为 180 s，可用 **undo peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]或 **undo peer** { *group-name* | *ipv4-address* | *ipv6-address*} **timer keepalive hold** [**min-holdtime**] 命令恢复 keepalive 消息的存活时间和保持时间为缺省值

14.10.3 配置 BGP 更新报文定时器

BGP 协议不会定期更新整个路由表，但当路由变化时会通过发送 Update（更新）报文向其对等体增量地更新路由表。这样可以设置发送 Update 报文的最小时间，通过减小更新报文发送周期，BGP 可以更快速地检测到路由变化，有利于 BGP 网络快速收敛。但是过短的更新报文时间会导致网络中的 Update 消息增多，使得设备的负担加重，并且会占用一定的网络带宽。

增大更新报文发送周期时间，可以减轻设备负担并减少网络带宽的占用，避免不必要的路由振荡。但是过长的保持时间会导致网络中的 Update 消息减少，使得 BGP 不能及时检测到路由的变化，不利于 BGP 网络快速收敛，还可能会造成流量损失。

BGP 更新报文定时器的配置方法很简单，只需在 BGP 视图下通过 **peer** { *group-name* | *ipv4-address* } **route-update-interval** *interval* 命令配置向对等体（组）发送相同路由前缀更新报文（Update 报文）的时间间隔即可。命令中的参数 *ipv4-address* | *group-name* 分别用来指定要设置发送更新报文的对等体或对等体组；参数 *interval* 指定发送 BGP 更新报文的最小时间间隔，取值范围是 0～600 的整数秒。

缺省情况下，IBGP 对等体的路由更新时间间隔为 15 s，EBGP 对等体的路由更新时间间隔为 30 s，可用 **undo peer** { *group-name* | *ipv4-address* } **route-update-interval** 命令恢复发送路由更新的时间间隔为缺省值。

【**示例**】配置向对等体发送路由更新的时间间隔为 10 s。

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.2 as-number 200
[Huawei-bgp] peer 1.1.1.2 route-update-interval 10
```

14.10.4 配置 EBGP 连接快速复位

EBGP 连接快速复位功能缺省情况下是使能的，目的是为了使 BGP 不必等待保持时间定时器超时，而立即快速响应接口故障，删除接口上的 EBGP 直连会话，便于 BGP 快速收敛。

但是如果 EBGP 连接所使用的接口状态反复变化，EBGP 会话就会反复重建与删除，造成网络振荡。这时，可以去使能 EBGP 连接快速复位功能，使 BGP 等待保持时间定时器超时才会删除接口上的 EBGP 直连会话。这样就在一定程度上抑制了 BGP 网络振荡，同时在一定程度上节约了网络带宽。

配置 EBGP 连接快速恢复的方法是在 BGP 视图下通过 **undo ebgp-interface-sensitive** 命令配置的。但 EBGP 连接快速复位功能只能快速响应接口故障，而不能快速响应接口故障恢复。接口故障恢复后，BGP 依靠自身状态机制来恢复会话。该命令适用于 EBGP 连接所使用的接口状态不断变化的场合。

缺省情况下，EBGP 连接快速复位功能是使能的，可通过 **ebgp-interface-sensitive** 命令进行使能。如果接口状态恢复稳定，建议立即执行 **ebgp-interface-sensitive** 命令恢复缺省配置，使能 EBGP 连接快速复位功能。

14.11　配置 BGP 安全性

通过配置 BGP 对等体的连接认证和配置 BGP GTSM 功能，可以提高 BGP 网络的安全性。具体可包括以下项配置。在配置 BGP 安全性之前，需配置 BGP 的基本功能。**配置认证时，要求对等体两端所配置的认证方式和认证密码完全一致。**

① 配置 MD5 认证。

② 配置 Keychain 认证。

③ 配置 BGP GTSM 功能。

14.11.1　配置 MD5 认证

BGP 使用 TCP 作为传输协议，只要 TCP 数据包的源地址、目的地址、源端口、目的端口和 TCP 序号是正确的，BGP 就会认为这个数据包有效，但数据包的大部分参数对于攻击者来说是不难获得的。

为了保证 BGP 免受攻击，可以在 BGP 邻居之间使用 MD5 认证或者 Keychain 认证来降低被攻击的可能性。其中 MD5 算法配置简单，配置后生成单一密码，需要人为干预才可以切换密码，适用于需要短时间加密的网络。如果 MD5 认证失败，则不建立 TCP 连接。**另外，BGP MD5 认证与 BGP Keychain 认证互斥**，不能在同一对等体或者对等体上配置。

MD5 认证的配置方法是在 BGP 视图下通过 **peer** { *ipv4-address* | *group-name* } **password** { **cipher** *cipher-password* | **simple** *simple-password* }命令配置 MD5 认证密码（**两端的认证方式和密码必须完全一致**）。命令中的参数说明如下。

① *ipv4-address* | *group-name*：指定要进行 MD5 认证的对等体 IP 地址或对等体组名称。

② **cipher** *cipher-password*：二选一参数，指定 MD5 密文密码，不允许空格，区分大小写，可以输入 1～255 个字符的明文，也可以输入 20～392 个字符的密文。

③ **simple** *simple-password* 二选一参数，指定 MD5 明文密码，1～255 个字符，不允许空格，区分大小写。

注意 在配置 MD5 认证密码时，如果使用 **simple** 选项，密码将以明文形式保存在配置文件中，存在安全隐患。建议使用 **cipher** 选项，将密码加密保存在配置文件中。

在采用输入明文方式来指定明文密码或密文密码字符串时，不支持以“$@$@”或“^#^#”同时作为起始和结束字符。

缺省情况下，BGP 对等体在建立 TCP 连接时对 BGP 消息不进行 MD5 认证，可用 **undo peer** { *group-name* | *ipv4-address* } **password** 命令恢复缺省情况。

【示例】配置对本地设备与对等体 1.1.1.2 之间的 TCP 连接使用认证。

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.2 as-number 200
[Huawei-bgp] peer 1.1.1.2 password simple huawei
```

14.11.2 配置 Keychain 认证

Keychain 认证方式具有一组密码，可以根据配置自动切换，安全性较 MD5 认证方式更高，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。配置 BGP Keychain 认证前，必须配置 *keychain-name* 对应的 Keychain 认证，否则 TCP 连接不能正常建立。

注意 BGP 对等体两端必须都配置针对使用 TCP 连接的应用程序的 Keychain 认证，所使用的 Keychain（密钥链）需已使用 **keychain** *keychain-name* 命令创建，然后分别通过 **key-id** *key-id* 、**key-string** { [**plain**] *plain-text* | [**cipher**] *cipher-text* } 和 **algorithm** { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }命令配置该 keychain 采用的 key-id、密码及其认证算法，必须保证本端和对端的 key-id、algorithm、key-string 相同，才能正常建立 TCP 连接，交互 BGP 消息。且 BGP Keychain 认证与 BGP MD5 认证与互斥，不能在同一对等体间同时配置。

配置 BGP Keychain 认证的方法是在 BGP 视图下使用 **peer** { *ipv4-address* | *group-name* } **keychain** *keychain-name* 命令进行的。命令中的 *ipv4-address* | *group-name* 是用来指定要进行 Keychain 认证的对等体 IP 地址或对等体组名称，参数 *keychain-name* 用来指定所采用的 Keychain 名称，1～47 个字符，区分大小写，不支持空格。

【示例】为对等体配置名为 Huawei 的 Keychain 认证。

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.2 as-number 200
[Huawei-bgp] peer 1.1.1.2 keychain Huawei
```

14.11.3 配置 BGP GTSM 功能

BGP GTSM（Generalized TTL Security Mechanism，通用 TTL 安全保护机制）是通过检测 IP 报文头中的 TTL 值是否在一个预先设置好的特定范围内，并对不符合 TTL 值范围的报文进行允许通过或丢弃的操作，从而实现了保护 IP 层以上业务，增强系统安全性的目的。

例如将 IBGP 对等体的报文的 TTL 的范围设为 254 至 255。当攻击者模拟合法的 BGP 报文，对设备不断地发送报文进行攻击时，TTL 值必然小于 254。如果没有使能 BGP GTSM 功能，设备收到这些报文后，发现是发送给本机的报文，会直接上送控制层面处理。这时将会因为控制层面处理大量攻击报文，导致设备 CPU 占用率高，系统异常繁忙。如果使能 BGP GTSM 功能，系统会对所有 BGP 报文的 TTL 值进行检查。丢弃 TTL 值小于 254 的攻击报文，从而避免了网络攻击报文占用 CPU。

BGP GTSM 功能的配置步骤如表 14-30 所示。

表 14-30　**BGP GTSM 功能的配置步骤**

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
3	**peer** { *group-name* | *ipv4-address* } **valid-ttl-hops** [*hops*] 例如：[Huawei-bgp] **peer** gtsm-group **valid-ttl-hops** 1	在 BGP 对等体（组）发来的报文检查上应用 GTSM 功能。但 **GTSM 只会对匹配 GTSM 策略的报文进行 TTL 检查**。且 GTSM 的配置是对称的，**需要在 BGP 连接的两端同时使能 GTSM 功能。也不能在同一对等体（组）上同时配置 peer** { *group-name* | *ipv4-address* } **ebgp-max-hop** [*hop-count*]命令，即不允许建立非直连的 EBGP 连接。命令中的参数说明如下 ● *group-name* | *ipv4-address*：指定要使能 GTSM 功能的对等体组名称或对等体 IP 地址 ● *hops*：指定需要检测的 TTL 跳数值，取值范围为 1～255 的整数，缺省值是 255，被检测的报文的 TTL 值有效范围为[255-*hops*+1, 255] 缺省情况下，BGP 对等体（组）上未配置 GTSM 功能，可用 **undo peer** { *group-name* | *ipv4-address* } **valid-ttl-hops** 命令撤销在指定 BGP 对等体（组）上应用的 GTSM 功能
4	**quit** 例如：[Huawei-bgp] **quit**	退出 BGP 视图，返回系统视图
5	**gtsm default-action** { **drop** | **pass** } 例如：[Huawei] **gtsm default-action drop**	（可选）设置没有匹配 GTSM 策略的报文的缺省动作。命令中的选项说明如下 ● **drop**：二选一选项，指定未匹配 GTSM 策略的报文不能通过过滤，报文被丢弃。对于丢弃的报文，可以通过下一步将要介绍的 **gtsm log drop-packet** 命令打开日志信息开关，控制是否对报文被丢弃的情况记录日志，以方便故障的定位 ● **pass**：二选一选项，指定未匹配 GTSM 策略的报文通过过滤 如果仅仅通过 **gtsm default-action** 命令配置了缺省动作，但没有配置 GTSM 策略（**drop** 或 **pass**）时，GTSM 功能不起作用 缺省情况下，未匹配 GTSM 策略的报文可以通过过滤，可用 **undo gtsm default-action drop** 命令取消未匹配 GTSM 策略的报文不能通过过滤的设置
6	**gtsm log drop-packet [all]** 例如：[Huawei] **gtsm log drop-packet**	（可选）打开当前单板（目前仅支持主控板，不支持接口板）或所有单板（选择 **all** 可选项时）的 LOG 信息开关，在单板 GTSM 丢弃报文时记录 LOG 信息 缺省情况下，在单板 GTSM 丢弃报文时不记录 LOG 信息，可用 **undo gtsm log drop-packet [all]**命令关闭所有或者指定单板 LOG 信息的开关

14.12 BGP 与 BFD 联动

BGP 通过周期性地向对等体发送 Keepalive 报文来实现邻居检测。但这种机制检测到故障所需的时间比较长，超过 1 s（缺省为 3 分钟）。当数据达到吉比特速率级时，这么长的检测时间将导致大量数据丢失，无法满足电信级网络高可靠性的需求。

14.12.1 配置 BGP 与 BFD 联动

为了解决 BGP 自身的故障检测速度慢的问题，BGP 与前面介绍的 RIP、OSPF 等协议一样，也可以通过与 BFD 联动实现更加快速的链路故障检测能力。BFD 检测是毫秒级，可以在 50 ms 内通报 BGP 对等体间链路的故障，因此能够提高 BGP 路由的收敛速度，保障链路快速切换，减少流量损失。

BGP 与 BFD 联动的配置步骤如表 14-31 所示（**需在 BFD 链路两端的设备上同时配置**）。

说明 当对等体加入了对等体组，且这个对等体组使能了 BFD 特性，则对等体将继承该对等体组的 BFD 特性，创建 BFD 会话。如果不希望对等体从对等体组继承 BFD 特性，可以配置 **peer bfd block** 命令，阻止对等体从对等体组中继承 BFD 功能。

表 14-31　　BGP 与 BFD 联动的配置步骤

步骤	命令	说明
1	**system-view** 例如：< Huawei > **system-view**	进入系统视图
2	**bfd** 例如：[Huawei] **bfd**	使能全局 BFD 能力
3	**quit** 例如：[Huawei-bfd] **quit**	退出 BFD 视图，返回系统视图
4	**bgp** { *as-number-plain* | *as-number-dot* } 例如：[Huawei]**bgp** 100	启动 BGP，进入 BGP 视图。命令中的参数说明参见 14.6.1 小节表 14-7 中的第 2 步
5	**peer** { *group-name* | *ipv4-address* } **bfd enable** 例如：[Huawei-bgp] **peer** 2.2.2.9 **bfd enable**	配置与对等体（组）的建立 BFD 功能，使用缺省的 BFD 参数值建立 BFD 会话。命令中的 *group-name* | *ipv4-address* 用来指定要建立 BFD 会话的对等体组名称或对等体 IP 地址 缺省情况下，没有使能与对等体（组）的 BFD 会话，可用 **undo peer** { *group-name* | *ipv4-address* } **bfd enable** 命令去使能与指定对等体（组）建立 BFD 会话
6	**peer** { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier*| **wtr** *wtr-value* } * 例如：[Huawei-bgp] **peer** 2.2.2.9 **bfd min-tx-interval** 100 **min-rx-interval** 100 **detect-multiplier** 5	指定需要建立 BFD 会话的各个参数值。命令中的参数说明如下 ● *group-name* | *ipv4-address*：指定要配置 BFD 会话参数的对等体组名称或对等体 IP 地址 ● **min-tx-interval** *min-tx-interval*：可多选参数，指定 BFD 发送检测报文的时间间隔，取值范围为 10～2 000 的整数毫秒 ● **min-rx-interval** *min-rx-interval*：可多选参数，指定 BFD 接收检测报文的时间间隔，取值范围为 10～2 000 的整数毫秒

（续表）

步骤	命令	说明
6	**peer** { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier*| **wtr** *wtr-value* } * 例如：[Huawei-bgp] **peer** 2.2.2.9 **bfd min-tx-interval** 100 **min-rx-interval** 100 **detect-multiplier** 5	• **detect-multiplier** *multiplier*：可多选参数，指定本地检测时间倍数，取值范围为 3～50 的整数 • **wtr** *wtr-value*：可多选参数，指定等待 BFD 会话恢复的时间，取值范围为 1～60 的整数分钟。缺省值是 0，表示不等待 【说明】本命令是覆盖式命令，若多次配置该命令，BFD 会话使用新的参数作为检测参数。如果同时在对等体以及它所属的对等体组上配置了 BFD 参数，则建立的 BFD 会话以对等体上的配置为准 具体参数如何配置取决于网路状况以及对网络可靠性的要求，对于网络可靠性要求较高的链路，可以配置减小 BFD 报文实际发送时间间隔；对于网络可靠性要求较低的链路，可以配置增大 BFD 报文实际发送时间间隔 • 本地 BFD 检测报文实际发送时间间隔＝MAX {本地配置的发送时间间隔 *transmit-interval*，对端配置的接收时间间隔 *receive-interval* } • 本地 BFD 检测报文实际接收时间间隔＝MAX {对端配置的发送时间间隔 *transmit-interval*，本地配置的接收时间间隔 *receive-interval* } • 本地 BFD 检测报文实际检测时间＝本地实际接收时间间隔×对端配置的 BFD 检测时间倍数 *multiplier-value* 缺省情况下，BFD 发送检测报文的时间间隔为 1 000 ms，BFD 接收检测报文的间隔为 1 000 ms，本地检测时间倍数为 3，可用 **undo peer** { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* | **wtr** *wtr-value* }* 命令恢复指定的 BFD 检测参数为缺省值
7	**peer** *ipv4-address* **bfd block** 例如：[Huawei-bgp] **peer** 2.3.3.9 **bfd block**	（可选）阻止对等体从对等体组中继承 BFD 功能。参数 *ipv4-address* 用来指定要阻止从所属的对等体组继承 BFD 功能的对等体 IP 地址 缺省情况下，对等体从对等体组中继承 BFD 功能，可用 **undo peer** *ipv4-address* **bfd block** 命令恢复指定对等体从对等体组中继承 BFD 功能

14.12.2 BGP 与 BFD 联动配置示例

本示例的基本拓扑结构如图 14-26 所示，RouterA 属于 AS100，RouterB 和 RouterC 属于 AS200，路由器 RouterA 和 RouterB，RouterA 和 RouterC 建立**非直连**（中间还经过了其他设备）的 EBGP 连接。正常情况下，业务流量在主链路 RouterA→RouterB 上传送，链路 RouterA→RouterC→RouterB 作为备份链路。现要求实现故障的快速感知，从而使得在主链路发生故障时流量从主链路能快速切换至备份链路进行转发。

说明　如果 RouterA 与 RouterB，或者 RouterC 之间使用的是直连链路建立 EBGP 邻居，

则无需配置 BGP 与 BFD 联动功能，因为 BGP 已经缺省配置了 **ebgp-interface-sensitive** 命令快速感知链路故障。当 EBGP 链路出现故障时，BGP 可以迅速感知并立即尝试使用其他接口复位原接口上的 BGP 连接。

1. 基本配置思路分析

BGP 与 BFD 联动功能的配置是在 BGP 基本功能配置之后进行的，需要在监控链路两端的 RouterA 与 RouterB 上分别配置 BGP 与 BFD 联动功能。另外，需要将 RouterB 的 MED 属性值配置得更小（因为 MED 属性是用来确定离开 AS 的路由路径的），以便正常情况下以及在主链路故障恢复后，最终选择从 RouterA→RouterB 的主链路进行数据转发。当然首先也要配置各路由器接口 IP 地址。

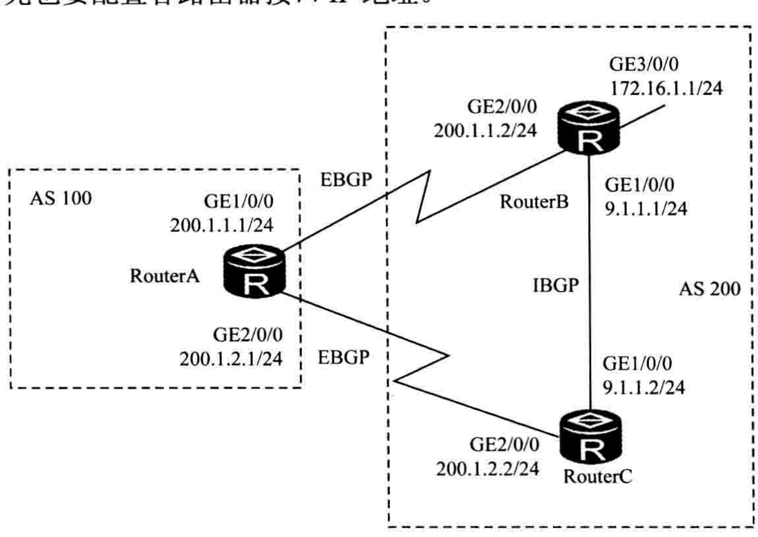


图 14-26 BGP 与 BFD 联动配置示例拓扑结构

2. 具体配置步骤

① 配置各路由器接口的 IP 地址。下面仅以 RouterA 上的接口为例进行介绍，其他路由器各接口的 IP 地址的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 200.1.1.1 24
[RouterA-GigabitEthernet1/0/0]quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 200.1.2.1 24
[RouterA-GigabitEthernet2/0/0]quit
```

② 配置各路由器的 BGP 基本功能，在 RouterA 和 RouterB、RouterA 和 RouterC 之间建立 EBGP 连接，RouterB 和 RouterC 之间建立 IBGP 连接。另外，**因为 RouterA 与 RouterB 之间，以及 RouterA 与 RouterC 之间建立的是非直连 EBGP 连接，所以在它们之间建立 EBGP 连接时一定要用 peer ebgp-max-hop 命令允许建立非直连 EBGP 连接。**

同样因本示例没有配置 Loopback 接口，所以需要明确配置各路由器的 Router ID。这是因为在没有明确配置路由器 ID 的情况下是优先以 Loopback 接口 IP 地址作为路由器 ID 的。为方便记忆，RouterA、RouterB、RouterC 的路由器 ID 分别设为 1.1.1.1、2.2.2.2、3.3.3.3。

RouterA 上的配置如下。

```
[RouterA] bgp 100
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.1.2 as-number 200
[RouterA-bgp] peer 200.1.1.2 ebgp-max-hop   !---指定与 RouterB 之间允许建立非直连 EBGP 连接
[RouterA-bgp] peer 200.1.2.2 as-number 200
[RouterA-bgp] peer 200.1.2.2 ebgp-max-hop
[RouterA-bgp] quit
```

RouterB 上的配置如下。

```
[RouterB] bgp 200
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.1.1 as-number 100
[RouterB-bgp] peer 200.1.1.1 ebgp-max-hop
[RouterB-bgp] peer 9.1.1.2 as-number 200
[RouterB-bgp] network 172.16.1.0 255.255.255.0
[RouterB-bgp] quit
```

RouterC 上的配置如下。要求同时引入它所连接的 172.16.1.0/24 直连网络，主要用于后面的验证。

```
[RouterC] bgp 200
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.2.1 as-number 100
[RouterC-bgp] peer 200.1.2.1 ebgp-max-hop
[RouterC-bgp] peer 9.1.1.1 as-number 200
[RouterC-bgp] import-route direct
[RouterC-bgp] quit
```

配置基本 BGP 功能后，可通过 **display bgp peer** 命令查看各路由器上已建立的 BGP 连接。下面是 RouterA 的输出示例，从中可以看出 RouterA 已与 RouterB 和 RouterC 分别建立了 EBGP 连接（Established）（**参见输出信息粗体字部分**）。

```
<RouterA> display bgp peer
 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Total number of peers : 2                 Peers in established state : 2

  Peer            V    AS   MsgRcvd   MsgSent   OutQ   Up/Down        State PrefRcv

  200.1.1.2       4    200        2         5      0 00:01:25 Established       0
  200.1.2.2       4    200        2         4      0 00:00:55 Established       0
```

③ 在 RouterB 和 RouterC 上分别通过路由策略配置发送给它们的对等体 RouterA 的 MED 属性，把 RouterB 上的 MED 属性值设为更小些，以便在正常情况下，以及当主链路故障恢复时 RouterA 能及时地恢复主链路的数据转发。

RouterB 上的配置如下。

```
[RouterB] route-policy 10 permit node 10
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] bgp 200
[RouterB-bgp] peer 200.1.1.1 route-policy 10 export
```

RouterC 上的配置如下。

```
[RouterC] route-policy 10 permit node 10
```

```
[RouterC-route-policy] apply cost 150
[RouterC-route-policy] quit
[RouterC] bgp 200
[RouterC-bgp] peer 200.1.2.1 route-policy 10 export
```

此时再在 RouterA 上通过 **display bgp routing-table** 命令查看 BGP 路由表。从中可以看出，去往 172.16.1.0/24 的路由下一跳地址为 200.1.1.2，流量在主链路 RouterA→RouterB 上传输（**参见输出信息粗体字部分**）。

```
<RouterA> display bgp routing-table
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,   i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 5
      Network            NextHop        MED         LocPrf    PrefVal Path/Ogn
 *>   9.1.1.0/24         200.1.2.2      150                   0       200?
 *>   172.16.1.0/24      200.1.1.2      100                   0       200i
 *                       200.1.2.2      150                   0       200i
 *>   200.1.2.0          200.1.1.2      100                   0       200?
                         200.1.2.2      150                   0       200?
```

④ 在 RouterA 和 RouterB 上分别配置 BFD 检测功能，配置相同的 BFD 报文的发送和接收间隔（本示例均为 100 ms），以及本地检测时间倍数参数（本示例均为 4）。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bgp 100
[RouterA-bgp] peer 200.1.1.2 bfd enable
[RouterA-bgp] peer 200.1.1.2 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4

[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bgp 200
[RouterB-bgp] peer 200.1.1.1 bfd enable
[RouterB-bgp] peer 200.1.1.1 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
```

此时可通过 **display bgp bfd session all** 命令在 RouterA 上查看 BGP 建立的所有 BFD 会话。

```
<RouterA> display bgp bfd session all
  Local_Address      Peer_Address      LD/RD        Interface
  200.1.1.1          200.1.1.2         8201/8201    GigibitEthernet1/0/0
  Tx-interval(ms)    Rx-interval(ms)   Multiplier   Session-State
  100                100               4            Up
  Wtr-interval(m)
  0
```

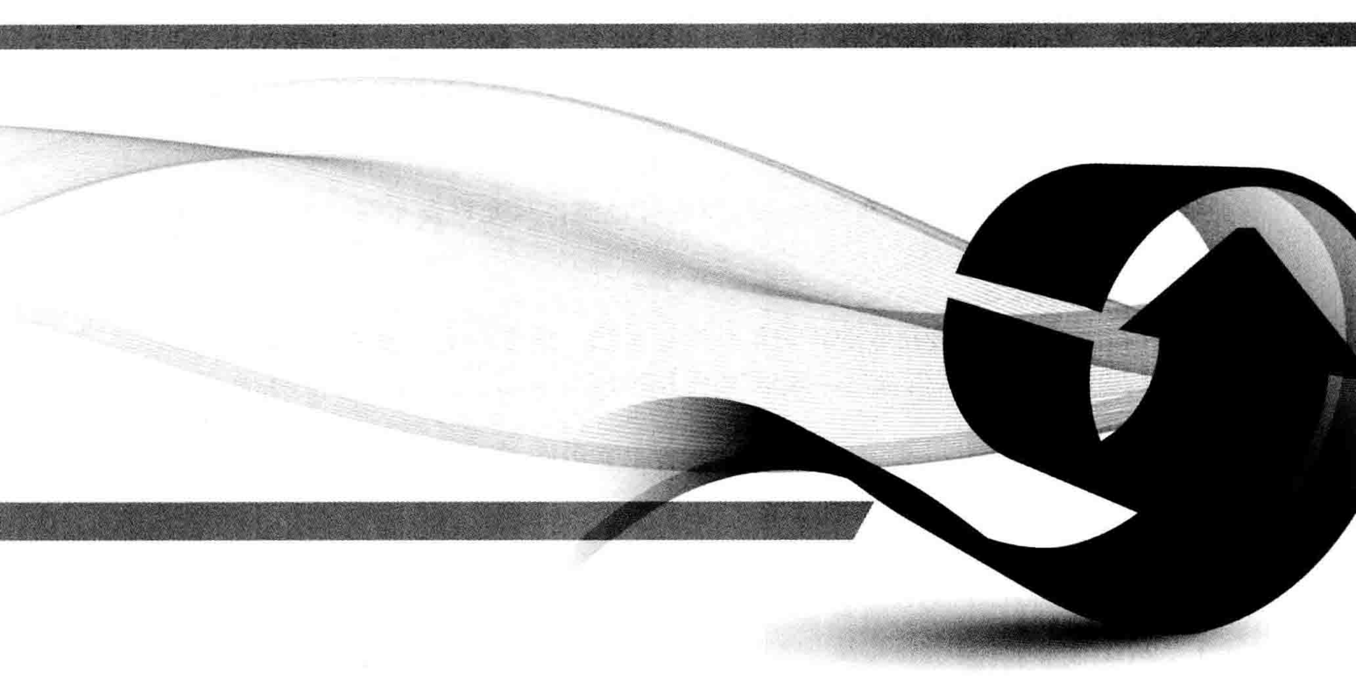
最后对 RouterB 的 GE2/0/0 接口执行 **shutdown** 命令，模拟主链路故障。然后在 RouterA 上通过 **display bgp routing-table** 命令查看其 BGP 路由表。从中可以看出，在主链路失效后，备份链路 RouterA→RouterC→RouterB 生效，去往 172.16.1.0/24 的路由下一跳地址为 200.1.2.2（**参见输出信息粗体字部分**）。达到了目的，证明以上配置是成功的。

```
<RouterA> display bgp routing-table
```

```
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history,   i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 3
      Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
*>  9.1.1.0/24           200.1.2.2       150                   0       200?
*>  172.16.1.0/24        200.1.2.2       150                   0       200i
    200.1.2.0            200.1.2.2       150                   0       200?
```

第15章 路由策略和策略路由配置与管理



“路由策略”和“策略路由”是路由业务中经常谈论的话题，也是日常的路由器配置与管理中最常用的两项综合技术，在本书前面各章也经常提到。许多读者朋友虽然知道它们不是一回事，但却说不出它们之间到底有什么区别，更不知道它们是如何应用的。

其实“路由策略”与“策略路由”之间的区别就在于它们的主体（或者叫“作用对象”）不同，前者的主体是“路由”，是对符合条件的路由（主要）通过修改路由属性来执行相应的策略动作（如允许通过、拒绝通过、接收、引入等），使通过这些路由的数据报文按照规定的策略进行转发；而后者的主体是数据报文，是对符合条件的数据报文（如报文的源地址、报文长度等）按照策略规定的动作进行操作（如设置报文的出接口和下一跳、设置报文的缺省出接口和下一跳等），然后转发。

本章将要介绍的“路由策略”其实在本书前面介绍的各种动态路由（包括RIP路由、OSPF路由、IS-IS路由和BGP路由）中已有具体的应用介绍，如这些动态路由信息发送（发布）/接收控制、路由选路、路由引入以及BGP路由属性配置等都用到了“路由策略”，本章将对“路由策略”在这些方面的应用进行全面的总结。另外，本章还将具体介绍AR G3系列路由器在“策略路由”方面的相关知识及应用配置方法，同时给出一些典型的应用配置示例，以加深对应用配置方法的理解。

15.1 路由策略基础

路由策略（Routing Policy）是通过使用不同的匹配条件和匹配模式来选择路由，或改变路由属性。路由策略主要应用在路由信息发布、接收、引入和路由属性修改等几个方面，具体如下。

1. 控制路由的发布

可通过路由策略对所要发布的路由信息进行过滤，只允许发布满足条件的路由信息。

2. 控制路由的接收

可通过路由策略对所要接收的路由信息进行过滤，只允许接收满足条件的路由信息。这样可以控制路由条件的数量，提高网络的路由效率。

3. 控制路由的引入

可通过路由策略只引入满足条件的路由信息，并控制所引入的路由信息的某些属性，使其满足本路由协议的路由属性要求。

4. 设置路由的属性

修改通过路由策略过滤的路由的属性，满足自身需要。

15.1.1 路由策略原理

要实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则，这就是路由策略中必须使用的过滤器（将在下节介绍，它们可以单独使用，也可组合使用）。可以用路由信息中的不同属性作为过滤器的匹配依据，如路由的目的地址、源地址等。然后将匹配规则应用于路由的发布、接收和引入等过程的策略中。

在一个路由策略中可以包括多组以 **if-match** 语句指定的匹配条件，这些匹配条件是以节点（Node）来进行标识的。如果在一个路由策略中包括多个节点，则路由会按照节点号从小到大依次进行匹配，直到与某节点的条件完全匹配（后面的节点就不再去匹配了），如果到了路由策略中所包括的最后一个节点仍没有完全匹配，则该路由拒绝通过。**不同节点间是逻辑“或”的关系**，即如果通过了其中一个节点，就意味着通过该路由策略，不再对其他节点进行匹配。

每个节点可以由一组 **if-match** 和 **apply** 子句组成。

① **if-match** 子句定义匹配规则，匹配对象是路由信息的一些属性。**同一节点中的不同 if-match 子句是逻辑“与”的关系**，即只有满足节点内所有 **if-match** 子句指定的匹配条件，才能通过该节点的匹配测试。

② **apply** 子句指定动作，也就是对通过节点匹配的路由信息进行属性设置。

【经验之谈】if-match 和 **apply** 子句可以根据应用进行设置，但都是可选的。如果只过滤路由，不设置路由的属性，则仅需配置 **if-match** 子句，不需要使用 **apply** 子句；如果某个 **permit** 节点没有配置任何 **if-match** 子句，则该节点匹配所有的路由；通常在多个 **deny** 节点后配置一个不含 **if-match** 子句和 **apply** 子句的 **permit** 节点，用于允许其他的路由通过。

如图 15-1 所示，一个路由策略中包含 *N* 个节点（Node）。当接收或者发送的路由要应用该路由策略时，会按节点序号从小到大依次检查与各个节点是否匹配。匹配条件由 **if-match** 子句定义，涉及路由信息的属性和路由策略的 6 种过滤器（具体将在下节介绍）。匹配模式分 **permit** 和 **deny** 两种。

① **permit**：表示该路由将被允许通过，并且执行该节点的 **apply** 子句对路由信息的一些属性进行设置。

② **deny**：表示该路由将被拒绝通过。

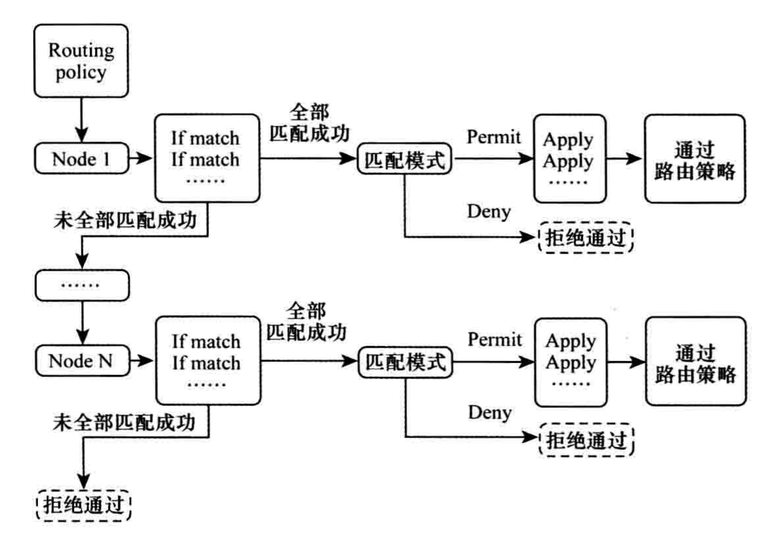


图 15-1　路由策略工作原理示意图

当路由与某节点的**所有 if-match** 子句都匹配成功后，进入匹配模式选择，不再匹配其他节点。当路由与该节点的**任意一个 if-match** 子句匹配失败后，进入下一节点。如果该路由与所有节点都匹配失败，则该路由信息将被拒绝通过。

15.1.2　路由策略过滤器

路由策略的实现是通过各种过滤器进行路由过滤完成的。在路由策略中，**if-match** 子句中匹配的 6 种过滤器包括访问控制列表 ACL（Access Control List）、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器和 RD 属性过滤器。这 6 种过滤器具有各自的匹配条件及 **permit** 和 **deny** 匹配模式，因此这 6 种过滤器在以下的特定情况中可以单独使用，实现路由过滤。

说明　过滤器可以看作是路由策略过滤路由的工具，但单独配置的过滤器没有任何过滤效果，只有在路由协议的相关命令中应用这些过滤器，才能够达到预期的过滤效果。

1．ACL

ACL 是将报文中的入接口、源或目的地址、协议类型、源或目的端口号作为匹配条件的过滤器，在各路由协议发布、接收路由时单独使用。但在路由策略中的 **if-match** 子**句只支持基本 ACL，过滤的是路由的目的 IP 地址和子网掩码**。有关 ACL 的详细介绍请

参见配套图书《华为交换机学习指南》。

2. 地址前缀列表

地址前缀列表（IP Prefix List）将路由的目的地址和子网掩码前缀作为匹配条件的过滤器（与 ACL 过滤器的作用是一样的），可在各路由协议发布和接收路由时单独使用。根据匹配的前缀不同，前缀过滤列表可以进行精确匹配，也可以在一定掩码长度范围内匹配。当 IP 地址为 0.0.0.0 时表示通配地址，表示掩码长度范围内的所有路由都被 Permit 或 Deny。

每个地址前缀列表可以包含多个索引（index），每个索引对应一个节点。路由按索引号从小到大依次检查各个节点是否匹配，任意一个节点匹配成功，将不再检查其他节点。若所有节点都匹配失败，路由信息将被过滤。

3. AS 路径过滤器

AS 路径过滤器（AS_Path Filter）是将 BGP 中的 AS_Path 属性作为匹配条件的过滤器，**专用于 BGP 路由过滤，在 BGP 发布、接收路由时单独使用**。AS_Path 属性记录了 BGP 路由经过的所有 AS 编号。有关 AS_Path 属性的详细介绍参见第 14 章。

4. 团体属性过滤器

团体属性过滤器（Community Filter）是将 BGP 中的团体属性作为匹配条件的过滤器，**专用于 BGP 路由过滤，在 BGP 发布、接收路由时单独使用**。BGP 的团体属性用来标识一组具有共同性质的路由。有关团体属性的详细介绍请参见第 14 章。

5. 扩展团体属性过滤器

扩展团体属性过滤器（Extcommunity Filter）是将 BGP 中的扩展团体属性作为匹配条件的过滤器，**专用于 VPN 网络中的 BGP 路由过滤**，可在 VPN 配置中利用 VPN Target 区分路由时单独使用。

目前，扩展团体属性过滤器仅适用于对 VPN 中的 VPN Target 属性的匹配。VPN Target 属性在 BGP/MPLS IP VPN 网络中控制 VPN 路由信息在各 Site 之间的发布和接收。

6. RD 属性过滤器

RD 团体属性过滤器（Route Distinguisher Filter）是将 VPN 中的 RD 属性作为匹配条件的过滤器，可在 VPN 配置中利用 RD 属性区分路由时单独使用。

VPN 实例通过路由标识符 RD 实现地址空间独立，区分使用相同地址空间的前缀。

15.1.3 路由策略配置任务

在路由策略配置中，主要包括以下三大配置任务。

① 配置要使用的对应过滤器。路由策略过滤器包括 ACL、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器和 RD 属性过滤器，可选择其中的一种或多种。

②（可选）创建一个路由策略，并通过 **if-match** 子句调用第一项配置任务中所配置的对应过滤器，定义路由策略所需匹配的条件。如果不配置本步骤，则表示所有路由在对应路由策略节点匹配成功，直接按照节点的匹配模式进行处理。

③（可选）最后可通过 **apply** 子句定义路由策略的动作，用来为匹配成功的路由设置对应的路由属性。如果不配置本步骤，则对应路由策略节点仅起过滤路由的作用，不

会对通过的路由进行任何属性设置。

15.2　配置路由策略过滤器

本章仅介绍常用的地址前缀列表、AS 路径过滤器、团体属性过滤器的配置。有关 ACL（路由策略中仅可使用基本 ACL）的配置方法参见配套图书《华为交换机学习指南》。

15.2.1　配置地址前缀列表

当需要根据路由的目的地址控制路由的发布和接收时，可配置地址前缀列表。地址前缀列表可以单独使用，也就是不在路由策略 **if-match** 语句中被调用，但这时地址前缀列表中要至少配置一个节点的匹配模式是 **permit**，否则所有路由将都被用于 IP 地址的过滤。

1. 地址前缀列表的配置

配置 IPv4 地址前缀列表的方法是在系统视图下使用 **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ipv4-address mask-length* [**match-network**] [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]命令。命令中的参数和选项说明如下。

① *ip-prefix-name*：指定地址前缀列表名称，唯一标识一个 IPv4 地址前缀列表，为 1～169 个字符，区分大小写，不支持空格。

② *index-number*：可选参数，标识地址前缀列表中的一条匹配条件的索引号，取值范围为 1～4 294 967 295 的整数。缺省情况下，该序号值按照配置先后顺序依次递增，每次加 10，第一个序号值为 10，值越小越优先被匹配。同一个名称的地址前缀列表最多可支持配置 65 535 个索引号。

③ **permit**：二选一选项，指定由参数 *index-number* 标识的匹配条件的匹配模式为允许模式。在该模式下，如果过滤的 IP 地址在定义的范围内，则通过过滤，进行相应的设置；否则，必须进行下一节点的测试。

④ **deny**：二选一选项，指定由参数 *index-number* 标识的匹配条件的匹配模式为拒绝模式。在该模式下，如果过滤的 IP 地址在定义的范围内，则该 IP 地址不能通过过滤，从而不能进入下一节点的测试；否则，将进行下一节点的测试。

⑤ *ipv4-address mask-length*：指定用来进行路由匹配的网络 IP 地址和掩码长度，*mask-length* 的取值范围为 0～32。如果将本参数指定为 0.0.0.0 0，则代表所有路由。

⑥ **match-network**：可选项，指定匹配网络地址，仅在 *ipv4-address* 参数值为 0.0.0.0 时才可以配置，用来匹配指定网络地址的路由。例如：**ip ip-prefix** prefix1 **permit** 0.0.0.0 8 可以匹配掩码长度为 8 的所有路由；而 **ip ip-prefix** prefix1 **permit** 0.0.0.0 8 **match-network** 可以匹配目的 IP 地址在 0.0.0.1～0.255.255.255 范围内的所有路由。

说明　一般情况下，IP 地址的网络 ID 不能为 0，但是在华为产品中可以支持网络 ID 为 0，而主机 ID 不为 0 的 IP 地址。但这种 IP 地址需要特殊的系统提供支持，所以此可选项实际上是极少使用的。

⑦ **greater-equal** *greater-equal-value*：可选参数，指定掩码长度可以匹配范围的下限（也即最小长度），取值限制为 *mask-length*≤*greater-equal-value*≤*less-equal-value*≤32。如果没有配置下面将要介绍的 **less-equal** *less-equal-value* 可选参数，则路由的掩码长度范围可在 *greater-equal-value* 和 32 之间。如果同时不配置 **greater-equal** *greater-equal-value* 和 **less-equal** *less-equal-value* 可选参数，则仅匹配 *mask-length* 参数指定的掩码长度路由。

⑧ **less-equal** *less-equal-value*：可选参数，指定掩码长度匹配范围的上限，取值限制为 *mask-length*≤*greater-equal-value*≤*less-equal-value*≤32。如果没有配置 **greater-equal** *greater-equal-value* 可选参数，则掩码长度范围在 *mask-length* 和 *less-equal-value* 之间。如果同时不配置 **greater-equal** *greater-equal-value* 和 **less-equal** *less-equal-value*，则使用 *mask-length* 作为掩码长度的路由。

【经验之谈】如果地址前缀列表中的所有条件都是 **deny** 模式，则任何路由都不能通过该过滤列表。这种情况下，建议在多条 **deny** 模式的条件后定义一条 **permit** 0.0.0.0 0 **less-equal** 32 条件，允许其他所有 IPv4 路由信息通过。

缺省情况下，系统中无 IPv4 地址前缀列表，可用 **undo ip ip-prefix** *ip-prefix-name* [**index** *index-number*] 命令删除指定的 IPv4 地址前缀列表。

配置完成后，可执行 **display ip ip-prefix** [*ip-prefix-name*]任意视图命令查看 IPv4 地址前缀列表的详细配置信息；也可通过 **reset ip ip-prefix** [*ip-prefix-name*]用户视图命令清除 IPv4 地址前缀列表统计数据。

2. 地址前缀列表的应用

地址前缀列表既可以作为过滤器被各种路由协议使用，也可以和路由策略配合使用，具体表现如下（除了与路由策略配置使用的命令外，其他命令均在本书对应章中已有相应的介绍）。

① 本命令通过与下列命令配合使用，可以以地址前缀列表为过滤条件对全局发布的路由信息进行过滤。

- 全局过滤发布的 RIP 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]
- 全局过滤发布的 OSPF 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]
- 全局过滤发布的 IS-IS 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]
- 全局过滤发布的 BGP 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

② 本命令通过与下列命令配合使用，可以以地址前缀列表为过滤条件对全局接收的路由信息进行过滤。

- 全局过滤接收的 RIP 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]
- 全局过滤接收的 OSPF 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**] } **import**
- 全局过滤接收的 IS-IS 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* |

ip-prefix *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

- 全局过滤接收的 BGP 路由：**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**

③ 本命令通过与 **peer** { *group-name* | *ipv4-address* } **ip-prefix** *ip-prefix-name* { **import** | **export** }命令配合使用，为特定的 BGP 对等体配置基于地址前缀列表的过滤器进行路由过滤。

④ 以地址前缀列表为过滤条件控制 IS-IS 的 Level-1 路由向 Level-2 区域进行路由渗透：**import-route isis level-1 into level-2** [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *。

⑤ 以地址前缀列表为过滤条件控制 IS-IS 的 Level-2 路由向 Level-1 区域进行路由渗透：**import-route isis level-2 into level-1** [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *。

⑥ 本命令通过与 **if-match ip-prefix** *ip-prefix-name* 命令在路由策略中配合使用，以地址前缀列表将作为路由匹配的条件，对接收或发送的路由进行测试。

3. 地址前缀列表的应用情形

同一个地址前缀列表可包含多个匹配条件，一个条件指定一个地址前缀范围。此时，多个条件之间是“**或**”的关系，**即通过其中任何一个条件就可通过该地址前缀列表的过滤；没有通过任何一个条件的过滤就意味着没有通过该地址前缀列表的过滤，都将被 Deny**。

地址前缀范围包括两个部分，分别由 *mask-length* 和[*greater-equal-value*，*less-equal-value*]决定。如果同时指定了这两部分，则要被过滤的 IP 地址必须匹配这两部分规定的前缀范围。*ipv4-address* 参数值为 0.0.0.0 时表示通配地址。此时不论掩码指定为多少，都表示掩码长度范围内的所有路由全部被 Permit 或 Deny。

现假设有如下 5 条路由：1.1.1.1/24、1.1.1.1/32、1.1.1.1/26、2.2.2.2/24 和 1.1.1.2/16，通过使用以下不同的地址前缀列表，进行过滤的结果不同。

（1）单条件匹配（即地址前缀列表中只有一个匹配条件）

单节点匹配时，根据匹配模式的不同又有以下两种匹配情形。

① Permit 模式：假设配置的命令为 **ip ip-prefix** aa **index** 10 **permit** 1.1.1.1 24，则匹配的结果是路由 1.1.1.1/24 被 Permit，其他都被 Deny。

这种情况属于单节点的精确匹配，此时只有路由的目的地址，掩码与地址列表中匹配条件完全相同的路由才会匹配成功，节点的匹配模式为 **Permit**，所以路由 1.1.1.1/24 被 Permit，属于匹配成功并被 Permit。本示例中的其他 4 条路由由于未匹配成功被 Deny。

② Deny 模式：如果配置的命令为 **ip ip-prefix** aa **index** 10 **deny** 1.1.1.1 24，则匹配的结果是本示例中的所有 5 条路由全部被 Deny。

这种情况依然属于单节点的精确匹配，但节点的匹配模式为 **deny**，所以路由 1.1.1.1/24 还是被 Deny，属于匹配成功但被 Deny，本示例中的其他 4 条路由则属于未匹配成功被默认 Deny。

（2）多条件匹配（即地址前缀列表中有多个节点的匹配条件）

根据所配置的匹配条件的不同，多条件匹配又有如下几种情形。

① 多节点：假设地址前缀列表中配置了以下两个节点，则匹配的结果是路由 1.1.1.1/24 被 Deny，路由 1.1.1.1/32 被 Permit，本示例中的其他 4 条路由都被 Deny。

```
ip ip-prefix aa index 10 deny 1.1.1.1 24
ip ip-prefix aa index 20 permit 1.1.1.1 32
```

这种情况属于多节点的精确匹配，即路由 1.1.1.1/24 在匹配节点 10 时，满足匹配条件，但匹配模式是 **deny**，所以属于匹配成功但被 Deny；而路由 1.1.1.1/32 在匹配节点 10 时，不满足匹配条件，则继续匹配节点 20，此时匹配成功，且节点 20 的匹配模式是 **permit**，所以属于匹配成功并被 Permit；而本示例中的其他三条路由由于都不符合节点 10 和 20 的条件，属于未匹配成功被默认 Deny。

② 只指定子网掩码长度和掩码长度上限：假设地址前缀列表配置为 **ip ip-prefix** aa **index** 10 **permit** 1.1.1.1 24 **less-equal** 32，则表示配置结果为 *greater-equal-value*=24、*less-equal-value*=32，此时的匹配结果为路由 1.1.1.1/24、1.1.1.1/26、1.1.1.1/32 均被 Permit，本示例中的其他两条路由被 Deny。

说明 在这种情形中，配置时要注意，各掩码长度参数必需满足以下条件：*mask-length*≤*greater-equal-value*≤*less-equal-value*，否则配置不成功。

③ 只指定子网掩码长度和掩码长度下限：假设地址前缀列表配置为 **ip ip-prefix** aa **index** 10 **permit** 1.1.1.1 24 **greater-equal** 26，表示配置结果为 *greater-equal-value*=26、*less-equal-value*=32，此时的匹配结果是路由 1.1.1.1/26 和 1.1.1.1/32 这两条路由均被 Permit，本示例中的其他三条路由被 Deny。

④ 同时指定子网掩码长度、掩码长度下限和掩码长度上限：假设地址前缀列表配置为 **ip ip-prefix** aa **index** 10 **permit** 1.1.1.1 24 **greater-equal** 26 **less-equal** 32，则表示配置结果为 *greater-equal-value*=26、*less-equal-value*=32，此时的匹配结果为路由 1.1.1.1/26 和 1.1.1.1/32 这两条路由均被 Permit，本示例中的其他三条路由被 Deny。

【经验之谈】从上面两个例子可以看出，如果一个匹配条件中指定了 *greater-equal-value* 参数，而 *less-equal-value* 参数为最大值 32，则与仅指定相同的 *greater-equal-value* 参数值（不指定 *less-equal-value* 参数）的匹配条件的匹配结果是一样的。

（3）通配地址匹配

在地址前缀列表中，当匹配的路由目的 IP 地址为 0.0.0.0 时，代表为通配地址，它又会因为所配置的子网掩码长度参数的不同而有不同的匹配结果。

① 只指定子网掩码长度和掩码长度上限。

假设地址前缀列表配置为 **ip ip-prefix aa index** 10 **permit** 0.0.0.0 8 **less-equal** 32，则表示配置结果为 *greater-equal-value*=8、*less-equal-value*=32，由于 0.0.0.0 为通配地址，所以所有掩码长度在 8 到 32 之间的路由全部被 Permit，即匹配所有掩码长度在 8 到 32 之间的路由。对应本示例，最终的匹配结果为本示例中 1.1.1.1/24、1.1.1.1/26、1.1.1.1/32、2.2.2.2/24 和 1.1.1.2/16 这 5 条路由均被 Permit。

② 只指定子网掩码长度和掩码长度下限。

假设地址前缀列表中配置了以下两个节点，则表示配置结果为对于节点 10，*greater-equal-value*=24，*less-equal-value*=32，由于 0.0.0.0 为通配地址，即所有掩码长度在 24 到

32 之间的路由全部被 Deny；对于节点 20，greater-equal-value=0、less-equal- value=32，由于 0.0.0.0 为通配地址，所有其他路由全部被 Permit。对应本示例，最终的匹配结果为只有路由 1.1.1.2/16 被 Permit，其他 4 条路由均被 Deny。

```
ip ip-prefix aa index 10 deny 0.0.0.0 24 less-equal 32
ip ip-prefix aa index 20 permit 0.0.0.0 0 less-equal 32
```

③ 多节点匹配。

假设地址前缀列表中配置了以下两个节点，则表示配置结果为：对于节点 10，符合条件的路由 2.2.2.2/24 被 Deny，对于节点 20，本示例中的其他 4 条路由都被 Permit。即最终的匹配结果为除路由 2.2.2.2/24 外的其他路由被 Permit。

```
ip ip-prefix aa index 10 deny 2.2.2.2 24
ip ip-prefix aa index 20 permit 0.0.0.0 0 less-equal 32
```

下面再举 3 个具体的示例。

【示例 1】配置名为 p1 的地址前缀列表，只允许 10.0.192.0/8 网段内，掩码长度在 17 到 18 之间的路由通过。

```
<Huawei> system-view
[Huawei] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

【示例 2】配置名为 p3 的地址前缀列表，拒绝 0.0.0.1～0.255.255.255 范围内的所有路由通过，允许其他路由通过。

```
<Huawei> system-view
[Huawei] ip ip-prefix p3 index 10 deny 0.0.0.0 8 match-network
[Huawei] ip ip-prefix p3 index 20 permit 0.0.0.0 0 less-equal 32
```

【示例 3】配置名为 abc 的地址前缀列表，仅过滤掉 10.1.0.0/16、10.2.0.0/16、10.3.0.0/16 三个网段的路由，而其他网段的路由信息可以通过。

```
< Huawei > system-view
[Huawei] ip ip-prefix abc index 10 deny 10.1.0.0 16
[Huawei] ip ip-prefix abc index 20 deny 10.2.0.0 16
[Huawei] ip ip-prefix abc index 30 deny 10.3.0.0 16
[Huawei] ip ip-prefix abc index 40 permit 0.0.0.0 0 less-equal 32
```

15.2.2 配置 AS 路径过滤器

AS 路径过滤器是利用 BGP 路由携带的 AS-Path 列表对路由进行过滤。在不希望接收某些 AS 的路由时，可以利用 AS 路径过滤器对携带这些 AS 号的路由进行过滤。当网络环境比较复杂时，如果利用 ACL 或者地址前缀列表过滤 BGP 路由，则需要定义多个 ACL 或者前缀列表，配置比较繁琐。这时也可以使用 AS 路径过滤器。

1. AS 路径过滤器配置

在 BGP 中配置 AS 路径过滤器的方法是在系统视图下配置 **ip as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **deny** | **permit** } *regular-expression* 命令。这里涉及 AS 路径正则表达式，命令中的参数和选项说明如下。

① *as-path-filter-number*：二选一参数，指定 AS 路径过滤器号，取值范围为 1～256 的整数。

② *as-path-filter-name*：二选一参数，指定 AS 路径过滤器名称，1～51 个字符，区分大小写，不支持空格，**且不能都是数字**。

③ **deny**：二选一选项，指定 AS 路径过滤器的匹配模式为拒绝模式。

④ **permit**：二选一选项，指定 AS 路径过滤器的匹配模式为允许模式。

⑤ *regular-expression*：指定用于过滤 AS 路径的正则表达式，为 1～255 个字符。例如^200. *100$，表示匹配所有以 AS 200 开始、以 AS 100 结束的 AS 路径域。

缺省情况下，系统中无 AS 路径过滤器，可用 **undo ip as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } [{ **deny** | **permit** } *regular-expression*]命令删除指定的 AS 路径过滤器。

完成配置后，可执行 **display ip as-path-filter** [*as-path-filter-number* | *as-path-filter-name*]命令查看已配置的 AS 路径过滤器信息。

说明 本命令配置的 AS 路径过滤器可以在 **peer** { *group-name* | *ipv4-address* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **import** | **export** }命令中直接被调用，应用于路由过滤，又可以在路由策略中作为 **if-match as-path-filter** 命令的过滤条件。

在 AS 路径过滤器中，AS 路径过滤器号（名称）相同的本命令之间是“与”的关系，也就是必须同时匹配同一名称的 AS 路径过滤器中的所有条件才算最终匹配。而在同一个 AS 路径过滤器编号下，可以定义多条规则（Permit 或 Deny）。

2. 正则表达式

正则表达式描述了一种字符串匹配的模式，由普通字符（例如字符从 a 到 z）和特殊字符（或称“元字符”）组成。正则表达式作为一个模板，将某个字符模式与所搜索的字符串进行匹配。正则表达式一般具有以下功能。

① 检查字符串中符合某个规则的子字符串，并可以获取该子字符串。

② 根据匹配规则对字符串进行替换操作。

正则表达式由普通字符和特殊字符组成。

① 普通字符匹配的对象是普通字符本身。包括所有的大写和小写字母、数字、标点符号以及一些特殊符号。例如 a 匹配 abc 中的 a，202 匹配 202.113.25.155 中的 202，@匹配 xxx@xxx.com 中的@。

② 特殊字符配合普通字符匹配复杂或特殊的字符串组合。表 15-1 是对特殊字符及其语法意义的使用描述。

表 15-1　正则表达式特殊字符

特殊字符	功能	示例
^	匹配行首的位置	^10 匹配 10.10.10.1，不匹配 20.10.10.1
$	匹配行尾的位置	1$匹配 10.10.10.1，不匹配 10.10.10.2
*	匹配前面的字符或者子正则表达式（下面将介绍）0 次或多次	• 10*可以匹配 1、10、100、1 000、… • (10)*可以匹配空、10、1 010、101 010、…
+	匹配前面的字符或者子正则表达式 1 次或多次	• 10+可以匹配 10、100、1 000、… • (10)+可以匹配 10、1 010、101 010、…
?	匹配前面的字符或者子正则表达式 0 次或 1 次。但因为当前，在华为公司数据通信设备上输入？时，系统显示为命令行帮助功能，所以华为公司数据通信设备不支持正则表达式输入？特殊字符	• 10?可以匹配 1 或者 10 • (10)?可以匹配空或者 10

（续表）

特殊字符	功能	示例
.	匹配任意单个字符	• 0.0 可以匹配 0x0、020… • .oo.可以匹配 book、look、tool…
( )	一对圆括号内的正则表达式作为一个子正则表达式，匹配子表达式并获取这一匹配。**圆括号内也可以为空，即不包括圆括号内的字符**	100(200)+可以匹配 100 200 100 200 200…
x|y	匹配 x 或 y	• 100|200 匹配 100 或者 200 • 1(2|3)4 匹配 124 或者 134，而不匹配 1 234、14、1 224、1 334
[xyz]	匹配正则表达式中包含的任意一个字符	[123]匹配 255 中的 2
[^xyz]	匹配正则表达式中未包含的字符	[^123]匹配除 123 之外的任何字符
[a-z]	匹配正则表达式指定范围内的任意字符	[0-9]匹配 0 到 9 之间的所有数字
[^a-z]	匹配正则表达式指定范围外的任意字符	[^0-9]匹配所有非数字字符
_	用来匹配输入字符串的开始位置、结束位置的字符，可以匹配的一个字符包括：逗号“,”、左大括号“{”、右大括号“}”、左圆括号“(”、右圆括号“)”，或者一个空格	_2008_可以匹配 2008、空格 2008 空格、空格 2008、2008 空格、2008
\	转义字符。将下一个或两个*之间的字符（特殊字符或者普通字符）标记为普通字符	*匹配*

下面是一些常用的 AS 路径正则表达式。

① ^$：表示匹配的字符串为空，即 AS_PATH 为空，表示只匹配本地路由。

② .*：表示匹配任意字符串，即 AS_PATH 为任意，表示匹配所有路由。

③ ^100：表示匹配的字符串开始为 100，即 AS_PATH 最左边 AS 前 3 位（最后一个AS）为 100，后面可能还有 AS，表示匹配由 AS100 发来的所有路由，包括从 AS100 始发和由 AS100 转发的路由。

④ ^100_：表示匹配的字符串开始为 100，后面为符号，即 AS_PATH 最左边 AS（最后一个 AS）为 100，后面一定还有其他 AS，表示匹配由 AS100 转发（路径中至少有两个 AS）的路由。比较前一个表达式^100 可以看出，“_”可以和用来限制仅匹配由某 AS 转发的路由。

⑤ _100$：表示匹配的字符串最后为 100，即 AS_PATH 最右边 AS（起始 AS）为 100，表示匹配 AS100 始发的路由。

⑥ _100_：表示匹配的字符串中间有 100，即 AS_PATH 中间有 AS100，表示匹配经过 AS100，且在 AS 路径中，AS100 既不是第一个 AS，也不是最后一个 AS 的路由。

【示例 1】 创建序号为 1 的 AS 路径过滤器，允许 AS 路径中以 10 开始的路由通过。

```
<Huawei> system-view
[Huawei] ip as-path-filter 1 permit ^10
```

【示例 2】 创建序号为 2 的 AS 路径过滤器，允许 AS 路径中包含 20 的路由通过。

```
<Huawei> system-view
[Huawei] ip as-path-filter 2 permit [ 20 ]
```

【示例 3】 创建序号为 3 的 AS 路径过滤器，不允许 AS 路径中包含 30 的路由通过。

```
<Huawei> system-view
[Huawei] ip as-path-filter 3 deny [ 30 ]
[Huawei] ip as-path-filter 3 permit .*
```

15.2.3 配置团体属性过滤器

团体属性可以标识具有相同特征（如来自或经过同一个或多个 AS，具有相同的 MED 属性，具有相同有本地优先级属性等）的路由，而不用考虑零散路由前缀和繁多的 AS 号。团体属性过滤器与团体属性配合使用，可以在不便使用地址前缀列表和 AS 属性过滤器时降低路由管理难度。

例如某公司一国外分部只需要接收国内总部和邻国分部的路由，不需要接收其他国外分部的路由。此时只需为各国分部分配不同的团体属性，就可以方便地实现路由管理，而不用考虑每个国家内零散的路由前缀和繁多的 AS 号。有关团体属性的介绍请参见 14.3.7 小节。

团体属性过滤器有两种类型：基本团体属性过滤器和高级团体属性过滤器。**基本团体属性过滤器是对已配置的团体路由成员**根据其中的路由的团体属性类型进行路由过滤，属于粗放型过滤器；**而高级团体属性过滤器是通过正则表达式**对符合团体属性过滤条件的路由进行过滤，比基本团体属性过滤器匹配团体属性更灵活。

基本团体属性过滤器的配置方法是在系统视图下使用 **ip community-filter** { **basic** *comm-filter-name* | *basic-comm-filter-num* } { **permit** | **deny** } [*community-number* |*aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] &<1-20>命令进行的。

高级团体属性过滤器的配置方法是在系统视图下使用 **ip community-filter** { **advanced** *comm-filter-name* | *adv-comm-filter-num* } { **permit** | **deny** } *regular-expression* 命令进行的。

以上两命令的参数和选项说明如下。

① **basic** *comm-filter-name*：二选一参数，指定所配置的基本团体属性过滤器名称，1～51 个字符，区分大小写，但不能全是数字。

② *basic-comm-filter-num*：二选一参数，指定基本团体属性过滤器号，为 1～99 的整数。

③ **advanced** *comm-filter-name*：二选一参数，指定高级团体属性过滤器名称，1～51 个字符，区分大小写，且不能都是数字。

④ *adv-comm-filter-num*：二选一参数，指定高级团体属性过滤器号，取值范围为 100～199 的整数。

⑤ **deny**：二选一选项，指定团体属性过滤器的匹配模式为拒绝模式。

⑥ **permit**：二选一选项，指定团体属性过滤器的匹配模式为允许模式。

⑦ *community-number*：多选一参数，指定要过滤路由的整数形式团体号（**需要事先按照本书第 14 章 14.7.7 节创建对应的团体属性**），取值范围为 0～4 294 967 295 的整数。一条命令最多可以指定 20 个团体号（但与后面配置的选项类型有关，具体参见下面说明），包括下面将要介绍的冒号分隔形式配置的 *aa:nn* 团体号。

⑧ *aa:nn*：多选一参数，指定要过滤路由的冒号分隔形式团体号（**需要事先按照 14.7.7 小节创建对应的团体属性**），*aa* 和 *nn* 都是整数形式，取值范围均为 0～65 535。一条命令最多可以指定 20 个团体号（但与后面配置的选项类型有关，具体参见下面说明），包括上面介绍的整数形式配置的 *community-number* 团体号。在配置团体号时要注意以下几

个方面。

- 如果不配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 选项，则 *community-number* 和 *aa:nn* 一共可以指定 20 个。
- 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的一个选项，则 *community-number* 和 *aa:nn* 一共可以指定 19 个。
- 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的两个选项，则 *community-number* 和 *aa:nn* 一共可以指定 18 个。
- 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的三个选项，则 *community-number* 和 *aa:nn* 一共可以指定 17 个。
- 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 选项，则 *community-number* 和 *aa:nn* 一共可以指定 16 个。

⑨ **internet**：多选一选项，指定要过滤指定团体号中 **internet** 类型团体属性的路由，这是预定义的团体属性。缺省情况下，所有的路由都具有 **internet** 类型团体属性，可以被通告给所有的 BGP 对等体。

⑩ **no-advertise**：多选一选项，指定要过滤指定团体号中 **no-advertise** 类型团体属性的路由，具有此属性的路由在收到后，不能被通告给任何其他的 BGP 对等体。

⑪ **no-export**：多选一选项，指定要过滤指定团体号中 **no-export** 类型团体属性的路由，具有此属性的路由在收到后，不能被发布到本地 AS 之外。如果使用了联盟，则不能被发布到联盟之外，但可以发布给联盟中的其他子 AS。

⑫ **no-export-subconfed**：多选一选项，指定要过滤指定团体号中 **no-export-subconfed** 类型团体属性的路由，具有此属性的路由在收到后，不能被发布到本地 AS 之外，也不能发布到联盟中的其他子 AS。

⑬ *regular-expression*：指定用于路由过滤的团体属性正则表达式名称，1～255 个字符，支持空格，区分大小写。有关正则表达式参见 15.2.2 小节介绍。

缺省情况下，没有配置团体属性列表，以上基本团体属性过滤器和高级团体属性过滤器分别可用 **undo ip community-filter** { **basic** *comm-filter-name* | *basic-comm-filter-num* } [**permit** | **deny**] [*community-number* | *aa:nn* | **internet** | **no-export-subconfed**| **no-advertise** | **no-export**] &<1-20>、**undo ip community-filter** { **advanced** *comm-filter-name* | *adv-comm-filter-num* } [**permit** | **deny**] [*regular-expression*]命令删除指定的基本或高级团体属性过滤器。

完成配置后，可以执行 **display ip community-filter** [*basic-comm-filter-num* | *adv-comm-filter-num* | *comm-filter-name*]命令查看已配置的团体属性过滤器信息。

【示例 1】配置团体号为 1 的基本团体属性过滤器，允许 **internet** 类型团体属性的 BGP 路由信息通过。

```
<Huawei> system-view
[Huawei] ip community-list 1 permit internet
```

【示例 2】配置团体号为 100 的高级团体属性过滤器，允许团体属性值（为整数形式，或者 aa:nn 冒号分隔形式）以“10”开头的路由信息通过。

```
< Huawei > system-view
[Huawei] ip community-list 100 permit ^10
```

15.3 配置路由策略

路由策略用来根据路由信息的某些属性过滤路由信息，并改变与路由策略规则匹配的路由信息的属性。匹配条件可以使用上节几种过滤列表。要配置路由策略，首先要创建一个路由策略，然后创建策略中的具体节点（一个路由策略可以包括多个节点）。一个节点下可以配置以下子句配置路由策略匹配条件和操作动作（一个路由策略中可以包含多个匹配条件和操作动作）。

① **if-match** 子句：定义节点匹配规则，即路由信息通过当前路由策略所需满足的条件，匹配对象是路由信息的某些属性。

② **apply** 子句：指定路由策略动作，也就是在满足由 **if-match** 子句指定的过滤条件后所执行的一些属性配置动作，对路由的某些属性进行修改。

在配置路由策略之前，需要先配置过滤列表和对应的路由协议，并事先规划好路由策略的名称、节点序号、匹配条件以及要修改的路由属性值。

15.3.1 创建路由策略

一个路由策略可以包括多个节点，每一节点由一些 **if-match** 子句和 **apply** 子句组成。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义通过该节点过滤后进行的动作。**但路由策略节点之间的过滤关系是“或”的关系**，即通过一个节点的过滤就意味着通过该路由策略的过滤。若没有通过任一节点的过滤，则表示没有通过该路由策略的过滤。所以在一个路由策略中，至少有一个节点的匹配模式是 **permit**，否则所有路由将都被禁止通过。

路由策略的创建方法很简单，只需要在系统视图下使用 **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node* 命令即可。命令中的参数和选项说明如下。

① *route-policy-name*：指定要创建的路由策略的名称，用来唯一标识一个路由策略，为 1～40 个字符的字符串，区分大小写。如果该名称的路由策略不存在，则创建一个新的路由策略并进入它的 Route-Policy 视图。如果该名称的路由策略已经存在，则直接进入它的 Route-Policy 视图。

② **permit**：二选一选项，指定所定义的路由策略节点的匹配模式为允许模式。在该模式下，**当路由满足该节点的所有 if-match 子句时才被允许通过**，并执行该节点的 **apply** 子句；如路由项不满足该节点下任何一个 **if-match** 子句，将继续测试该路由策略的下一个节点。

③ **deny**：二选一选项，指定所定义的路由策略节点的匹配模式为拒绝模式。在该模式下，**当路由满足该节点的所有 if-match 子句时将被拒绝通过**；如路由不满足该节点下任何一个 **if-match** 子句，将继续测试该路由策略的下一个节点。

④ **node** *node*：标识路由策略中的一个节点号，节点号小的进行匹配，取值范围为 0～65 535 的整数。当一个节点匹配成功后，该路由将不再匹配其他节点。当全部节点匹配失败后，该路由将被过滤，不允许通过。

默认情况下，没有创建路由策略，可用 **undo route-policy** *route-policy-name* [**permit** |

deny] [**node** *node*]命令删除指定名称的路由策略或指定节点号策略。

说明 为了便于区分不同的路由策略，可以在路由策略视图下通过 **description** *text* 命令为路由策略配置描述信息。参数 *text* 指定路由策略的描述信息，1～80 个字符，支持空格，不支持符号“？”，区分大小写。

【示例】创建一个名为 policy1 的路由策略，其节点序列号为 10，匹配模式为 permit，并进入路由策略视图。

```
<Huawei> system-view
[Huawei] route-policy policy1 permit node 10
[Huawei-route-policy]
```

15.3.2　配置 if-match 子句

if-match 子句是路由策略中用来匹配条件的子句，它可以根据多种路由属性来进行匹配，如路由的目的 IP 地址、路由标记、路由下一跳、路由源 IP 地址、路由出接口、路由开销、路由类型、BGP 路由的团体属性、BGP 路由的扩展团体属性、BGP 路由的 AS 路径属性等。正因为如此，在路由策略中可以配置的 **if-match** 子句命令比较多，具体如表 15-2 所示。

注意 表中的各种 **if-match** 子句命令是并列关系，没有严格的先后次序，也不要求在具体的配置方案中配置所有这些命令，根据实际选择其中一个或几个 if-match 子句命令即可。但如果在同一路由策略节点下配置了多个 **if-match** 子句，则**各 if-match 子句之间是逻辑“与”关系，即必须与该节点下的所有 if-match 子句匹配成功**。

另外，对于同一个路由策略节点，表中的 **if-match acl** 命令和 **if-match ip-prefix** 命令不能同时配置，且后配置的命令会覆盖先配置的命令。

表 15-2　if-match 子句的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node* 例如：[Huawei]**route-policy** policy **permit node** 10	进入路由策略视图
3	**if-match acl** { *acl-number* | *acl-name* } 例如：[Huawei-route-policy] **if-match acl** 2000	（可选）匹配基本 ACL，创建一个基于 ACL 的匹配规则。命令中的参数说明如下 • *acl-number*：二选一参数，指定用于过滤路由信息目的 IP 地址及其对应的反掩码（也属于路由 IP 地址前缀过滤）的基本 ACL 的编号，取值范围是 2 000～2 999 的整数 • *acl-name*：二选一参数，指定用于过滤路由信息目的 IP 地址及其对应的反掩码的命名型 ACL 的名称，1～32 个字符，不支持空格，区分大小写。以英文字母 a～z 或 A～Z 开始，可以是英文字母、数字、连字符“-”或下划线“_”的组合。只有 **source** 参数指定的源地址范围（对应路由信息中的目的 IP 地址）和 **time-range** 参数指定的时间段对配置规则有效

（续表）

步骤	命令	说明
3	**if-match acl** { *acl-number* | *acl-name* } 例如：[Huawei-route-policy] **if-match acl** 2000	缺省情况下，路由策略中无基于 ACL 的匹配规则，可用 **undo if-match acl** { *acl-number* | *acl-name* }命令删除指定的基于 ACL 的匹配规则 【注意】本命令与下面将要介绍的 **if-match ip-prefix** 命令是互斥的，即后配置的 if-match ip-prefix 可以覆盖先前配置的本命令
	if-match ip-prefix *ip-prefix-name* 例如：[Huawei-route-policy] **if-match ip-prefix** p1	（可选）匹配地址前缀列表，创建一个基于 IP 地址前缀列表的匹配规则。命令中的 *ip-prefix-name* 参数用来指定用于过滤路由信息 IP 地址前缀（包括路由的目的网络 IP 地址和对应的子网掩码）的 IP 地址前缀列表名称，1～169 个字符，区分大小写，不支持空格 缺省情况下，路由策略中无 IP 地址前缀列表的匹配规则，可用 **undo if-match ip-prefix** *ip-prefix-name* 命令删除指定的基于 IP 地址前缀列表的匹配规则 【注意】本命令与上面介绍的 **if-match acl** 命令是互斥的，即后配置的 **if-match acl** 可以覆盖先前配置的本命令 如果指定的 IP 地址前缀列表没有配置，则当前路由都会被 Permit
	if-match as-path-filter { *as-path-filter-number* &<1-16>| *as-path-filter-name* } 例如：[Huawei-route-policy] **if-match as-path-filter** 2	匹配路由信息的 as-path 属性过滤器，创建一个基于 AS 路径过滤器的匹配规则。命令中的参数说明如下 ● *as-path-filter-number*：二选一参数，指定用于过滤路由的 AS 路径的过滤器号，取值范围为 1～256 的整数。在一个命令行中可以配置多个此参数，但最大不能超过 16 ● *as-path-filter-name*：二选一参数，指定用于过滤路由的 AS 路径的 AS 路径过滤器名称，1～51 个字符，区分大小写，不支持空格，且不能都是数字 缺省情况下，路由策略中无基于 AS 路径过滤器的匹配规则，可用 **undo if-match as-path-filter** [*as-path-filter-number* &<1-16> | *as-path-filter-name*]命令删除指定的基于 AS 路径过滤器的匹配规则 【注意】如果在一个节点中配置多条本命令子句，则各子句间是"或"的关系，但与其他命令的 if-match 子句间仍是"与"的关系 如果指定的 AS 路径过滤器没有配置，则当前路由都会被 Permit
	iif-match community-filter { *basic-comm-filter-num* [**whole-match**] | *adv-comm-filter-num* } &<1-16> 或 **if-match community-filter** *comm-filter-name* [**whole-match**] 例如：[Huawei-route-policy] **if-match community-filter** 1 **whole-match** 2 **whole-match**	（可选）匹配路由信息的团体属性过滤器，创建一个基于团体属性过滤器的匹配规则。命令中的参数和选项说明如下 ● *basic-comm-filter-num*：二选一参数，指定用于路由团体属性过滤的基本团体属性过滤器号，取值范围为 1～99 的整数。每条命令最多可配置 16 个基本团体属性过滤器 ● **whole-match**：可选项，表示要求完全匹配，即在团体属性过滤器中的团体属性与路由信息的团体属性必须完全一致，且完全匹配，但仅对基本团体属性过滤器生效。如果不选择本可选项，则只需要路由信息中的团体属性与团体属性过滤器中的对应属性匹配即可 ● *adv-comm-filter-num*：二选一参数，指定用于路由团体属性过滤的高级团体属性过滤器号，取值范围为 100～199 的整数。每条命令最多可配置 16 个高级团体属性过滤器

（续表）

步骤	命令	说明
3	**iif-match community-filter** { *basic-comm-filter-num* [**whole-match**] | *adv-comm-filter-num* } <1-16> 或 **if-match community-filter** *comm-filter-name* [**whole-match**] 例如：[Huawei-route-policy] **if-match community-filter** 1 **whole-match** 2 **whole-match**	• *comm-filter-name*：指定用于路由团体属性过滤的团体属性过滤器名称，1～51 个字符，区分大小写，不支持空格，且不能都是数字 缺省情况下，路由策略中无基于团体属性过滤器的匹配规则，可用 **undo if-match community-filter** [*basic-comm-filter-num* | *adv-comm-filter-num*] <1-16>，或者 **undo if-match community-filter** *comm-filter-name* 命令删除指定的基于团体属性过滤器的匹配规则 【说明】**whole-match** 选项只对其前面的一个团体过滤器号生效。当本命令中指定了多个基本团体过滤器，且要求每一个过滤器都必须完全匹配时，则需要在每个基本团体过滤器后面加上这个可选项
	if-match cost *cost* 例如： [Sysname-route-policy] **if-match cost** 40	（可选）匹配路由信息的开销值，创建一个基于路由开销的匹配规则。参数用来指定要过滤的路由开销值，取值范围为 0～4 294 967 295 的整数 缺省情况下，路由策略中无基于路由开销的匹配规则，可用 **undo if-match cost** 命令删除基于路由开销的匹配规则
	if-match interface { *interface-type interface-number* }<1-16> 例如：[Huawei-route-policy] **if-match interface** gigabitethernet 1/0/0	（可选）匹配路由信息的出接口，创建一个基于出接口的匹配规则。参数 *interface-type interface-number* 指定用于路由信息过滤的出接口，最多 16 个 缺省情况下，路由策略中无基于出接口的匹配规则，可用 **undo if-match interface** [*interface-type interface-number*] <1-16>命令删除指定的基于出接口的匹配规则
	if-match ip { **next-hop** | **route-source** | **group-address** } { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* } 例如：[Huawei-route-policy] **if-match ip route-source acl** 2000	（可选）匹配 IPv4 的路由信息（下一跳、源地址或组播组地址），创建一个基于 IP 信息的匹配规则。命令中的参数和选项说明如下。 • **next-hop**：多选一选项，指定要匹配路由信息的下一跳 • **route-source**：多选一选项，指定匹配的发布路由信息的源 IP 地址 • **group-address**：多选一选项，指定要匹配路由信息的组播组 IP 地址 • **acl** { *acl-number* | *acl-name* }：二选一参数，指定用于过滤以上 IP 信息的基本 ACL。对于命名型 ACL，使用 rule 命令配置过滤规则时，只有 **source** 参数指定的源地址范围和 **time-range** 参数指定的时间段对配置规则有效 • **ip-prefix** *ip-prefix-name*：二选一参数，指定用于过滤以上 IP 信息的 IP 地址前缀列表 缺省情况下，路由策略中无基于 IP 信息的匹配规则，可用 **undo if-match ip** { **next-hop** | **route-source** | **group-address** } [**acl** { *acl-number* | *acl-name* } | **ip-prefix** ip-prefix-name]命令删除指定的基于 IP 信息的匹配规则 【注意】当被过滤的路由下一跳或者路由源为 0.0.0.0 这种特殊路由时，系统默认其对应的掩码长度为 0 来进行匹配如果指定的 ACL 或者 IP 地址前缀列表没有配置，则当前路由都会被 Permit

（续表）

步骤	命令	说明
3	**if-match route-type { external-type1 | external-type1or2 | external-type2 | internal | nssa-external-type1 | nssa-external-type1or2 | nssa-external-type2 }** 例如：[Huawei-route-policy] **if-match route-type nssa-external-type1**	（可选）匹配 OSPF 各类型路由信息，创建一个基于 OSPF 路由类型的匹配规则。命令中的选项说明如下 ● **external-type1**：多选一选项，指定匹配 OSPF Type1 的外部路由 ● **external-type1or2**：多选一选项，指定同时匹配 OSPF Type1 或者 Type2 的外部路由 ● **external-type2**：多选一选项，指定匹配 OSPF Type2 的外部路由 ● **internal**：多选一选项，指定匹配 OSPF 内部路由（包括 OSPF 区域间和区域内路由） ● **nssa-external-type1**：多选一选项，指定匹配 OSPF NSSA Type1 的外部路由 ● **nssa-external-type1or2**：多选一选项，指定匹配 OSPF NSSA Type1 或者 Type2 的外部路由 ● **nssa-external-type2**：多选一选项，指定匹配 OSPF NSSA Type2 的外部路由 缺省情况下，路由策略中无基于 OSPF 路由类型的匹配规则，可用 **undo if-match route-type { external-type1 | external-type1or2 | external-type2 | internal | nssa-external-type1 | nssa-external-type1or2 | nssa-external-type2 }** 命令删除指定的基于 OSPF 路由类型的匹配规则 【说明】同一个路由策略节点内，后配置的本命令子句不会取代之前配置的本命令子句，而是同时生效。在匹配的过程中，各个本命令子句间是"或"的关系，即路由信息只要匹配条件之一，就可以执行 apply 子句的动作。例如：先配置了 **if-match route-type nssa-external-type1** 命令，然后配置 **if-match route-type external-type1** 命令，则表示 OSPF 的 NSSA Type1 外部路由或者 OSPF Type1 的外部路由都可以匹配上
	if-match route-type { is-is-level-1 | is-is-level-2 } 例如：[Huawei-route-policy] **if-match route-type is-is-level-1**	（可选）匹配 IS-IS 各 level 路由信息，创建一个基于 IS-IS 路由类型的匹配规则。命令中的选项说明如下 ● **is-is-level-1**：二选一选项，指定匹配 IS-IS 的 Level-1 路由 ● **is-is-level-2**：二选一选项，指定匹配 IS-IS 的 Level-2 路由 缺省情况下，路由策略中无基于 IS-IS 路由类型的匹配规则，可用 **undo if-match route-type { is-is-level-1 | is-is-level-2 }** 命令删除指定的基于 IS-IS 路由类型的匹配规则
	if-match tag *tag* 例如：[Huawei-route-policy] **if-match tag** 8	（可选）匹配路由信息的标记字段，创建一个基于路由信息标记（Tag）的匹配规则。命令中的参数用来指定匹配的路由信息标记值，取值范围为 0～4 294 967 295 的整数。路由标记可将路由按实际需求分类，同类路由打上相同的 Tag，在路由策略中根据 Tag 对路由进行灵活的控制和管理 缺省情况下，路由策略中无基于 Tag 的匹配规则，可用 **undo if-match tag** 命令删除基于 Tag 的匹配规则

15.3.3　配置 apply 子句

Apply 子句用来为路由策略指定动作，用来设置匹配成功的路由的属性。在一个节点中，如果没有配置 **apply** 子句，则该节点仅起过滤路由的作用。如果配置一个或多个 **apply** 子句，则通过节点匹配的路由将执行所有 **apply** 子句。

与上节介绍的各种 **if-match** 子句命令一样，也有许多不同动作的 **apply** 子句命令，具体如表 15-3 所示。同样，这些 **apply** 子句命令没有严格的先后次序，也不一定要全面配置，需根据实际需要选择其中一个或几个进行配置。

表 15-3　　apply 子句配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei>**system-view**	进入系统视图
2	**route-policy** *route-policy-name* {**deny** | **permit** } **node** *node-number* 例如：**[Huawei]route-policy** policy1 **permit node** 10	进入该路由策略视图
3	**apply as-path** { *as-number-plain* | *as-number-dot* } &<1-10> { **additive** | **overwrite** } 或 **apply as-path none overwrite** 例如：[Huawei-route-policy] **apply as-path** 200 10.10 **additive**	（可选）在路由策略中配置改变 BGP 路由的 AS_Path 属性的动作。当 BGP 路由需要改变 AS_Path 属性来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的 BGP 路由的 AS_Path 属性。当到达同一目的地存在多条路由时，BGP 会比较路由的 AS_Path 属性，AS_Path 列表较短的路由将被认为是最佳路由。**通过替换 AS_Path 属性隐藏路由的真实路径信息，或者使原本两条不能形成负载分担的路由形成负载分担（替换后与另一个路由的 AS_Path 属性完全相同）**。AS 命令中的参数和选项说明如下 ● *as-number-plain*：二选一参数，对匹配成功的路由指定要替换或增加的整数形式的 AS 号，取值范围为 1～4 294 967 295 的整数。在同一个命令行中最多可以同时指定 10 个 AS 号 ● *as-number-dot*：二选一参数，对匹配成功的路由指定要替换或增加的点分形式的 AS 号，格式为 *x.y*，*x* 和 *y* 都是整数形式，*x* 的取值范围为 1～65 535，*y* 的取值范围为 0～65 535。在同一个命令行中最多可以同时指定 10 个 AS 号 ● **additive**：二选一选项，对匹配成功的路由指定在原有的 AS_Path 列表的最前面（即添加作为靠近本地 AS 的 AS 号列表）添加以上 *as-number-plain* | *as-number-dot* 参数指定的 AS 号 ● **overwrite**：二选一选项，对匹配成功的路由指定用以上 *as-number-plain* | *as-number-dot* 参数指定的 AS 号覆盖原有的 AS_Path 列表 ● **none overwrite**：对匹配成功的路由指定清空原来的 AS_Path 列表 缺省情况下，路由策略中未配置改变 BGP 路由的 AS_Path 属性的动作，可用 **undo apply as-path** 命令恢复缺省配置 【注意】策略生效后，会影响 BGP 路由选路。配置该命令会直接影响网络流量所经过的途径，另外也可能造成环路和选路错误，请谨慎使用该命令

（续表）

步骤	命令	说明
3	**apply backup-interface** *interface-type interface-number* 例如：[Huawei-route-policy] **apply backup-interface** gigabitethernet1/0/0	（可选）在路由策略中配置创建备份出接口的动作。该命令主要应用于 IP FRR（Fast ReRoute，快速重路由）场景，使用本命令可以手动为路由配置一个备份的出接口。在使能 IP FRR 功能之后，当主用链路发生故障，数据流量可以快速地切换到备份出接口。参数 *interface-type interface-number* 用来对匹配成功的路由指定备份出接口 【说明】本命令一般需要和下面将要介绍的 **apply backup-nexthop** 命令配合使用。但对于 P2P 链路，可以不设置备份下一跳；而对于非 P2P 链路，**必须设置备份下一跳** 缺省情况下，路由策略中未配置创建备份出接口的动作，可用 **undo apply backup-intreface** 命令恢复缺省配置
	apply backup-nexthop { *ipv4-address* | **auto** } 例如：[Huawei-route-policy] **apply backup-nexthop** 192.168.20.2	（可选）在路由策略中配置创建备份下一跳的动作。该命令主要应用于手动 IP FRR 和手动 VPN FRR 场景，使用本命令可以手动为路由配置一个备份的下一跳。在使能 IP FRR 功能之后，当主用链路发生故障时，数据流量可以快速地切换到备份下一跳 命令中的参数和选项说明如下 • *ipv4-address*：二选一参数，为匹配成功的路由指定备份下一跳的 IP 地址 • **auto**：二选一选项，为匹配成功的路由设置为自动寻找备份下一跳模式 缺省情况下，路由策略中未配置创建备份下一跳的动作，可用 **undo apply backup-nexthop** 命令恢复缺省配置
	apply comm-filter { *basic-comm-filter-number* | *adv-comm-filter-number* | *comm-filter-name* } **delete** 例如：[Huawei-route-policy] **apply comm-filter** 1 **delete**	（可选）在路由策略中配置删除指定团体属性过滤器中的团体属性的动作。当需要删除几个团体属性时，可通过一条团体属性过滤器配置命令将需要删除的团体属性分条配置到一个团体属性过滤器中，最后应用包含本命令的路由策略删除该团体属性过滤器中的所有团体属性。命令中的参数说明如下 • *basic-comm-filter-number*：多选一参数，指定要对匹配成功的 BGP 路由删除团体属性的基本团体属性过滤器号，取值范围为 1～99 的整数 • *adv-comm-filter-number*：多选一参数，指定要对匹配成功的 BGP 路由删除团体属性的高级团体属性过滤器号，取值范围为 100～199 的整数 • *comm-filter-name*：多选一参数，指定要对匹配成功的 BGP 路由删除团体属性的团体属性过滤器名称，1～51 个字符，区分大小写，不支持空格，且不能都是数字 【说明】当通过本命令删除指定的团体属性过滤器中的团体属性时，团体属性过滤器中的每条配置命令只能包含一个团体属性。如果要删除多个的团体属性值，必须先在同一团体属性过滤器下面配置多条团体属性配置命令 当在一个策略的同一个节点上同时配置了下面将要介绍的 **apply community** 命令和本命令时，**系统并不关注配置顺序，在执行设置操作之前先执行删除操作** 缺省情况下，路由策略中未配置删除指定团体属性过滤器中的团体属性的动作，可用 **undo apply comm-filter** 命令恢复缺省配置

（续表）

步骤	命令	说明
3	**apply community** { *community-number* | *aa:nn* | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } &<1-32> [**additive**] 或 **apply community none** 例如：[Huawei-route-policy] **apply community no-export**	（可选）在路由策略中配置改变 BGP 路由团体属性的动作，或者删除全部的 BGP 路由团体属性。当需要对 BGP 路由进行分类标识，更好地运用路由策略时，可以应用包含本命令的路由策略，设置匹配成功的 BGP 路由的团体属性。命令中的参数和选项说明如下 ● *community-number* | *aa:nn*：多选一参数，指定为匹配成功的路由改变团体属性的团体号（就是修改路由中的团体属性号）。一条命令中最多可以配置 32 个团体号，具体有以下几种配置 ➢ 如果不配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export**，则 *community-number* 和 *aa:nn* 一共可以指定 32 个 ➢ 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的一个，则 *community-number* 和 *aa:nn* 一共可以指定 31 个 ➢ 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的两个，则 *community-number* 和 *aa:nn* 一共可以指定 30 个 ➢ 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export** 中的三个，则 *community-number* 和 *aa:nn* 一共可以指定 29 个 ➢ 如果配置 **internet**、**no-export-subconfed**、**no-advertise** 和 **no-export**，则 *community-number* 和 *aa:nn* 一共可以指定 28 个 ● **internet**：多选一选项，为匹配成功的路由指定为 **internet** 类型团体属性，表示可以向任何对等体发送匹配的路由。缺省情况下，所有的路由都属于 internet 团体 ● **no-advertise**：多选一选项，为匹配成功的路由指定为 **no-advertise** 类型团体属性，表示不向任何对等体发送匹配的路由。即收到具有此属性的路由后，不能发布给任何其他的 BGP 对等体 ● **no-export**：多选一选项，为匹配成功的路由指定为 **no-export** 类型团体属性，表示不向 AS 外发送匹配的路由，但发布给其他子自治系统。即收到具有此属性的路由后，不能发布到本地 AS 之外 ● **no-export-subconfed**：多选一选项，为匹配成功的路由指定为 **no-export-subconfed** 类型团体属性，表示不向 AS 外发送匹配的路由，也不发布给其他子 AS。即收到具有此属性的路由后，不能发布给任何其他的子 AS ● **additive**：可选项，表示在原来路由的团体属性中追加由参数 *community-number* | *aa:nn* 指定的路由的团体属性。如果不选择本可选项，则是按照 *community-number* | *aa:nn* 参数值替换路由中原来的团体属性值 ● **none**：指定删除匹配成功的路由中的所有团体属性 缺省情况下，在路由策略中未配置改变 BGP 路由团体属性的动作，可用 undo apply community 命令恢复缺省配置

（续表）

步骤	命令	说明
3	**apply cost** [+ | -] *cost* 例如：[Huawei-route-policy] **apply cost** 120	（可选）在路由策略中配置改变路由的开销值的动作。当路由需要改变开销值来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的路由的开销值（**值越小，优先级越高**）。命令中的参数和选项说明如下 ● +：二选一可选项，指定对匹配成功的路由增加由后面 *cost* 参数配置的路由开销值 ● -：二选一可选项，指定对匹配成功的路由减少由后面 *cost* 参数配置的路由开销值。当同时不选择“+”和“-”选项时，后面是的 *cost* 参数是为匹配成功的路由设置指定的路由开销值 ● *cost*：对匹配成功的路由增加（选择“+”选项时），或者减少（选择“-”选项时），或者设置路由开销值，取值范围为 0～4 294 967 295 的整数 缺省情况下，在路由策略中未配置改变路由的开销值的动作，可用 **undo apply cost** 命令恢复缺省配置
	apply cost-type { **external** | **internal** } 例如：[Huawei-route-policy] **apply cost-type external**	（可选）在路由策略中配置改变 IS-IS 或者 BGP 路由的开销类型的动作。当路由需要改变开销类型来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的路由的开销类型。命令中的选项说明如下 ● **external**：二选一选项，指定匹配成功的 IS-IS 路由为外部路由开销类型 ● **internal**：二选一选项，指定匹配成功的 IS-IS 路由为内部路由开销类型，或者指定 BGP 路由的 MED 值为下一跳的 IGP 路由开销值。**Internal** 类型开销的路由优先于 **external** 类型开销的路由 缺省情况下，在路由策略中未配置改变路由的开销类型的动作，可用 **undo apply cost-type** 命令恢复缺省配置
	apply cost-type { **type-1** | **type-2** } 例如：[Huawei-route-policy] **apply cost-type type-1**	（可选）在路由策略中配置改变 OSPF 路由的开销类型的动作。当路由需要改变开销类型来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的路由的开销类型。命令中的选项说明如下 ● **type-1**：二选一选项，指定匹配成功的 OSPF 外部路由的开销类型为 Type-1，具有较高的可信度，这类外部路由的开销值=本设备到相应的 ASBR 的开销+ASBR 到该路由目的地址的开销 ● **type-2**：二选一选项，指定匹配成功的 OSPF 外部路由的开销类型为 Type-2，可信度较低，这类外部路由的开销值=ASBR 到该路由目的地址的开销。**type-1** 类型开销的 OSPF 路由优先于 **type-2** 类型开销的 OSPF 路由 缺省情况下，在路由策略中未配置改变路由的开销类型的动作，可用 **undo apply cost-type** 命令恢复缺省配置
	apply ip-address next-hop { *ipv4-address* | **peer-address** } 例如：[Huawei-route-policy] **apply ip-address next-hop** 193.1.1.8	（可选）在路由策略中配置改变 BGP 路由的下一跳地址的动作。当 BGP 路由需要改变下一跳地址来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的 BGP 路由的下一跳地址。命令中的参数说明如下 ● *ipv4-address*：二选一参数，为匹配成功的路由指定下一跳 IP 地址 ● **peer-address**：二选一选项，为匹配成功的路由指定 BGP 对等体地址为下一跳

（续表）

步骤	命令	说明
3	**apply ip-address next-hop** { *ipv4-address* | **peer-address** } 例如：[Huawei-route-policy] **apply ip-address next-hop** 193.1.1.8	缺省情况下，在路由策略中未配置改变BGP路由的下一跳地址的动作，可用 **undo apply ip-address next-hop** { *ipv4-address* | **peer-address** }命令删除指定的下一跳改变策略 【注意】通过策略设置路由信息的下一跳地址分两种情况 ● IBGP：对于 IBGP 对等体，配置的入口策略或者出口策略均可以生效。如果策略中配置的下一跳地址是不可达的，那么 IBGP 对等体也会将该路由加入 BGP 路由表中，但不是有效路由 ● EBGP：对于 EBGP 对等体，一般配置为入口策略。这是因为如果配置为出口策略，这条路由到达 EBGP 对等体后会因为下一跳不可达而被丢弃。当 EBGP 对等体是通过物理连接直接建立时，该策略不能生效，即路由信息的下一跳地址不发生改变
	apply dampening *half-life-reach reuse suppress ceiling* 例如：[Huawei-route-policy] **apply dampening** 20 2000 10000 16000	（可选）在路由策略中配置改变 EBGP 路由的衰减参数的动作。为了避免在 BGP 网络中频繁振荡路由对设备的影响，可以在 BGP 网络中使能衰减功能。应用包含本命令的路由策略，可以改变匹配成功的 BGP 路由的衰减参数。命令中的参数说明如下 ● *half-life-reach*：为匹配成功的可达路由指定半衰期，取值范围为 1～45 整数分钟 ● *reuse*：为匹配成功的路由指定解除抑制状态的阈值，取值范围为 1～20 000 的整数。当惩罚值降低到该值以下，路由就被再使用 ● *suppress*：为匹配成功的路由指定进入抑制状态的阈值，取值范围为 1～20 000 的整数，实际配置的值必须大于 *reuse* 的值。当惩罚值超过该极限时，路由受到抑制 ● *ceiling*：为匹配成功的路由指定惩罚上限值，取值范围为 1 001～20 000 的整数。实际配置的值必须大于 *suppress* 缺省情况下，在路由策略中未配置改变 EBGP 路由的衰减参数的动作，可用 **undo apply dampening** 命令恢复取消改变 EBGP 路由的衰减参数的动作 【注意】该命令中的各配置参数没有缺省值，必须显式配置。所指定的 *reuse*、*suppress*、*ceiling* 三个阈值是依次增大的，即必须满足：*reuse*<*suppress*<*ceiling*。根据公式 MaxSuppressTime=*half-life-reach*×60×(ln(*ceiling*/*reuse*)/ln(2))，如果 MaxSuppressTime 小于 1 就不能抑制。所以要保证 MaxSuppressTime 大于等于 1，即必须满足：*ceiling*/*reuse* 足够大
	apply isis { **level-1** | **level-1-2** | **level-2** } 例如：[Huawei-route-policy] **apply isis level-1**	（可选）在路由策略中配置改变引入到 IS-IS 协议中的路由的级别的动作。为避免 IS-IS 引入过多外部路由，给运行 IS-IS 的设备带来额外的负担，可以在 IS-IS 中引入路由时应用包含本命令的路由策略，改变引入 IS-IS 协议中的路由的 Level 级别。命令中的选项说明如下 ● **level-1**：多选一选项，指定匹配成功的引入 IS-IS 中的路由的级别为 Level-1 ● **level-1-2**：多选一选项，指定匹配成功的引入 IS-IS 中的路由的级别为 Level-1-2

（续表）

步骤	命令	说明
3	**apply isis** { **level-1** | **level-1-2** | **level-2** } 例如：[Huawei-route-policy] **apply isis level-1**	• **level-2**：多选一选项，指定匹配成功的引入 IS-IS 中的路由的级别为 Level-2 缺省情况下，在路由策略中未配置改变引入 IS-IS 协议中的路由的级别的动作，可用 **undo apply isis** 命令恢复缺省配置
	apply local-preference *preference* 例如：[Huawei-route-policy] **apply local-preference** 130	（可选）在路由策略中配置改变 BGP 路由信息的本地优先级的动作。当 BGP 路由需要改变离开 AS 的路径时，可以应用包含本命令的路由策略，改变匹配成功的 BGP 路由的本地优先级。当 BGP 网络中的路由器通过不同的 IBGP 对等体得到目的地址相同，但下一跳不同的多条路由时，将优先选择 Local_Pref 属性值较高的路由（**值越大，优先级越高**）。但本地优先级**仅用于同一个 AS 域内的选路，不向域外发布这个属性**。命令中的 *preference* 参数用来为匹配成功的 BGP 路由指定本地优先级，取值范围为 0～4 294 967 295 的整数 缺省情况下，在路由策略中未配置改变 BGP 路由信息的本地优先级的动作，可用 **undo apply local-preference** 命令取消改变 BGP 路由信息的本地优先级的动作
	apply origin { **egp** { *as-number-plain* | *as-number-dot* } | **igp** | **incomplete** } 例如：[Huawei-route-policy] **apply origin igp**	（可选）在路由策略中配置改变 BGP 路由的 Origin 属性的动作。当 BGP 路由需要改变 Origin 属性来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的 BGP 路由的 Origi 值。Origi 值是 BGP 协议的私有属性，该属性定义路径信息的来源。命令中的参数和选项说明如下 • **egp** { *as-number-plain* | *as-number-dot* }：多选一参数，指定匹配成功的 BGP 路由信息源为外部路由，优先级中等。其中 *as-number-plain* 为指定外部路由的整数形式 AS 号，*as-number-dot* 为指定外部路由的点分形式 AS 号，用于唯一标识一个 AS。当需要改变路由的来源为外部路由时，使用此参数 • **igp**：多选一选项，指定匹配成功的 BGP 路由信息源为内部路由，优先级最高。通过路由始发 AS 的 IGP（内部网关协议）得到的路由，例如使用 **network** 命令注入到 BGP 路由表的路由 • **incomplete**：多选一选项，指定匹配成功的 BGP 路由信息源为未知，优先级最低。通过其他方式学习到的路由信息，例如 BGP 通过 **import-route** 命令引入的路由，其 Origin 属性为 Incomplete 缺省情况下，在路由策略中未配置改变 BGP 路由的 Origin 属性的动作，可用 **undo apply origin** 命令恢复为缺省配置
	apply ospf { **backbone** | **stub-area** } 例如：[Huawei-route-policy] **apply ospf backbone**	（可选）在路由策略中配置将路由引入 OSPF 网络特定区域的动作。为避免 OSPF 引入过多外部路由，给运行 OSPF 的设备带来额外的负担，可以在 OSPF 引入路由时，应用包含本命令的路由策略来将路由引入 OSPF 网络的骨干区域或 NSSA 区域。命令中的选项说明如下 • **backbone**：二选一选项，表示将匹配成功的路由引入 OSPF 网络的骨干区域 • **stub-area**：二选一选项，表示将匹配成功的路由引入 OSPF 网络的 Stub 区域 缺省情况下，在路由策略中未配置将路由引入 OSPF 网络的特定区域的动作，可用 **undo apply ospf** 命令恢复为缺省配置

（续表）

步骤	命令	说明
3	**apply preference** *preference* 例如：[Huawei-route-policy] **apply preference** 90	（可选）在路由策略中配置改变路由的优先级的动作。当路由需要改变路由优先级来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的路由的优先级（**值越大，优先级越低**）。命令中的 *preference* 参数用来为匹配成功的路由指定优先级，取值范围为 1～255 的整数 缺省情况下，在路由策略中未配置改变路由的优先级的动作，可用 **undo apply preference** 命令恢复为缺省配置
	apply preferred-value *preferred-value* 例如：[Huawei-route-policy] **apply preferred-value** 66	（可选）在路由策略中配置改变 BGP 路由的首选值的动作。当 BGP 路由需要改变首选值来参与路由选择的竞争时，可以应用包含本命令的路由策略，改变匹配成功的 BGP 路由的首选值（**值越大，优先级越高**）。**但本命令配置本地生效，在 BGP 的出口策略中不生效**。命令中的参数 *preferred-value* 用来为匹配成功的路由指定首选值，取值范围为 0～65 535 的整数 缺省情况下，路由策略中未配置改变 BGP 路由的首选值的动作，可用 **undo apply preferred-value** 命令恢复为缺省配置
	apply tag *tag* 例如：[Huawei-route-policy] **apply tag** 100	（可选）在路由策略中配置改变路由信息标记（Tag）的动作。当需要对路由进行分类标识，更好地运用路由策略时，可以应用包含本命令的路由策略，将匹配成功的路由打上相同的 Tag。**但 BGP 没有 Tag 属性，本命令只能设置 IGP 路由信息的标记**。命令中的参数用 *tag* 来为匹配成功的路由信息指定标记值，取值范围为 0～4 294 967 295 的整数 缺省情况下，路由策略中未配置改变路由信息标记的动作，可用 **undo apply tag** 命令恢复为缺省配置

15.3.4 配置路由策略生效时间

为了保障网络的稳定性，修改路由策略时可以控制路由策略的生效时间，当然这是可选的配置任务，因为缺省是立即生效。具体的配置步骤如表 15-4 所示。

表 15-4　　路由策略生效时间的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**route-policy-change notify-delay** *delay-time* 例如：[Huawei]**route-policy-change notify-delay** 20	控制路由策略变化后 RM 通知各协议重新应用策略的延迟时间，取值范围为 1～180 的整数秒 【说明】当路由策略的相关命令配置变化后，缺省情况下，RM 会立即通知协议进行处理。如果不希望路由策略变化通知过快，可以根据实际情况，应用此命令配置延迟等待时间。路由策略将在定时器超时后应用新的策略 ● 如果在等待时间内路由策略的配置又发生了改变，RM 将重置定时器，重新开始计时 ● 如果新策略被 BGP 协议使用，那么在本命令配置的延迟时间内，仍可以通过执行下面将要介绍的 refresh bgp all 命令，触发 BGP 协议立即应用新策略

（续表）

步骤	命令	说明
2	**route-policy-change notify-delay** *delay-time* 例如：[Huawei]**route-policy-change notify-delay** 20	受该延时设置影响的相关的策略有 ACL、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器、RD 属性过滤器和 Route-Policy 配置命令 缺省情况下，没有配置此命令，应用新策略的延迟时间是 0 s，即立即生效，可用 **undo route-policy-change notify-delay** 命令取消设置，恢复为缺省值
3	**quit** 例如：[Huawei] **quit**	退出系统视图，返回用户视图
4	**refresh bgp all** { **export** | **import** } 例如：<Huawei> **refresh bgp all import**	（可选）配置 BGP 协议立即应用新策略，手工对 BGP 连接进行软复位。命令中的选项说明如下 ● **export**：二选一选项，表示触发出方向的软复位 ● **import**：二选一选项，表示触发入方向的软复位 【说明】如果配置策略命令后，需要立即看到策略过滤的效果。可以通过执行这个命令，配置 BGP 协议立即应用新策略。受该定时器影响的相关的策略有访问控制列表、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器、RD 属性过滤器和 Route-Policy

配置好路由策略后，可通过 **display route-policy** [*route-policy-name*]任意视图命令查看路由策略的详细配置信息。

15.3.5 AS_Path 过滤器配置示例

本示例的基本拓扑结构如图 15-2 所示，RouterA 与 RouterB、RouterB 与 RouterC 之间建立 EBGP 连接。用户希望 AS 10 的设备和 AS 30 的设备无法相互通信。

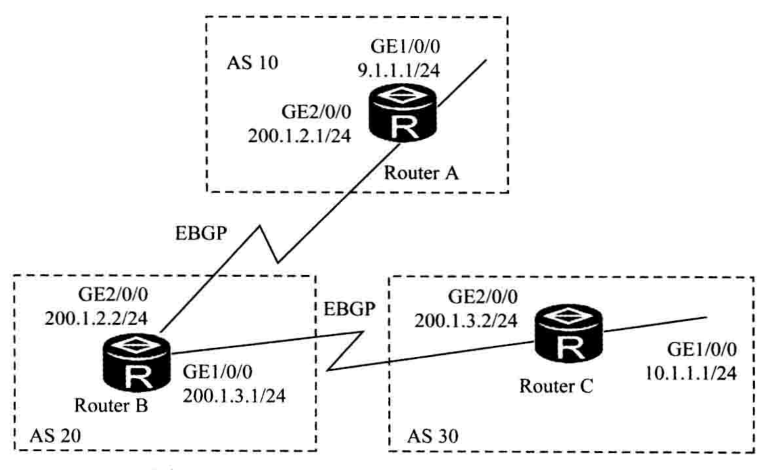


图 15-2 AS_Path 过滤器配置示例拓扑结构

1. 基本配置思路分析

本示例的配置比较简单，除了需要进行基本的 BGP 功能配置（配置 EBGP 对等体以及引入直连路由）外，还要在 RouterB 上配置一个 AS_Path 过滤器。可采用如下思路配置 BGP 的 AS_Path 过滤器，使 AS 20 不向 AS 10 发布 AS 30 的路由，也不向 AS 30

发布 AS 10 的路由。当然，首先还是要为各路由器接口配置 IP 地址。

2. 具体配置步骤

① 配置各接口的 IP 地址。下面仅以 RouterA 上的接口 IP 地址配置为例进行介绍，RouterB 和 RouterC 上的配置方法一样，略。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet1/0/0] ip address 200.1.2.1 24
```

② 配置各路由器的 EBGP 对等体连接，同时引入直连路由，以使它们彼此三层互通。因为本示例中没有配置 Loopback 接口，所以需要为它们分别配置路由器 ID。为了方便记忆，RouterA、RouterB 和 RouterC 的路由器 ID 分别设为 1.1.1.1、2.2.2.2 和 3.3.3.3。

RouterA 上的配置如下。

```
[RouterA] bgp 10
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.2.2 as-number 20
[RouterA-bgp] import-route direct
```

RouterB 上的配置如下。

```
[RouterB] bgp 20
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.2.1 as-number 10
[RouterB-bgp] peer 200.1.3.2 as-number 30
[RouterB-bgp] import-route direct
[RouterB-bgp] quit
```

RouterC 上的配置如下。

```
[RouterC] bgp 30
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.3.1 as-number 20
[RouterC-bgp] import-route direct
[RouterC-bgp] quit
```

配置好基本功能后，可以在各路由器上通过 **display bgp routing-table** 命令查看各处的 BGP 路由表。现以 RouterB 发布给 RouterC 的 BGP 路由表为例，从中可以看到 RouterB 除了发布自己引入的直连路由和从 RouterC 学习到的直连路由外，还向 RouterC 发布了 AS 10 引入的直连路由 9.1.1.0/24（**参见输出信息中的粗体字部分**）。

```
<RouterB> display bgp routing-table peer 200.1.3.2 advertised-routes
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 5
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         200.1.3.1                           0      20 10?
 *>   10.1.1.0/24        200.1.3.1                           0      20 30?
 *>   200.1.2.0          200.1.3.1      0                    0      20?
 *>   200.1.2.1/32       200.1.3.1      0                    0      20?
 *>   200.1.3.0/24       200.1.3.1      0                    0      20?
```

同样可以通过 **display bgp routing-table** 命令查看 RouterC 的 BGP 路由表，可以看到 RouterC 也通过 RouterB 学习到了 9.1.1.0/24 这条路由（**参见输出信息中的粗体字

部分）。

```
<RouterC> display bgp routing-table
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 9
      Network          NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24       200.1.3.1                           0      20 10?
 *>   10.1.1.0/24      0.0.0.0        0                    0      ?
 *>   10.1.1.1/32      0.0.0.0        0                    0      ?
 *>   127.0.0.0        0.0.0.0        0                    0      ?
 *>   127.0.0.1/32     0.0.0.0        0                    0      ?
 *>   200.1.2.0        200.1.3.1      0                    0      20?
 *>   200.1.3.0/24     0.0.0.0        0                    0      ?
 *                     200.1.3.1      0                    0      20?
 *>   200.1.3.2/32     0.0.0.0        0                    0      ?
```

③ 在 RouterB 上配置 AS_Path 过滤器，并在 RouterB 的出方向上应用该过滤器。

首先创建编号为 1 的 AS_Path 过滤器，拒绝包含 AS 号 30 的路由通过（正则表达式“_30_”表示任何包含 AS 30 的 AS 列表，“.*”表示与任何字符匹配）。

```
[RouterB] ip as-path-filter path-filter1 deny _30_
[RouterB] ip as-path-filter path-filter1 permit .*
```

然后，创建编号为 2 的 AS_Path 过滤器，拒绝包含 AS 号 10 的路由通过。

```
[RouterB] ip as-path-filter path-filter2 deny _10_
[RouterB] ip as-path-filter path-filter2 permit.*
```

最后，分别在 RouterB 的两个出方向上应用以上这两个 AS_Path 过滤器。

```
[RouterB] bgp 20
[RouterB-bgp] peer 200.1.2.1 as-path-filter path-filter1 export
[RouterB-bgp] peer 200.1.3.2 as-path-filter path-filter2 export
[RouterB-bgp] quit
```

此时，再通过 **display bgp routing-table** 命令查看 RouterB 发往 AS 30 的发布路由表。可以看到表中没有 RouterB 发布的 AS 10 引入的直连路由，表明过滤成功。

```
<RouterB> display bgp routing-table peer 200.1.3.2 advertised-routes
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 2
      Network          NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   200.1.2.0        200.1.3.1      0                    0      20?
 *>   200.1.3.0/24     200.1.3.1      0                    0      20?
```

同样，RouterC 的 BGP 路由表里也没有这些路由，具体如下。

```
<RouterC> display bgp routing-table
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
```

```
                 Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 8
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   10.1.1.0/24        0.0.0.0        0                    0       ?
 *>   10.1.1.1/32        0.0.0.0        0                    0       ?
 *>   127.0.0.0          0.0.0.0        0                    0       ?
 *>   127.0.0.1/32       0.0.0.0        0                    0       ?
 *>   200.1.2.0          200.1.3.1      0                    0       20?
 *>   200.1.3.0/24       0.0.0.0        0                    0       ?
 *                       200.1.3.1      0                    0       20?
 *>   200.1.3.2/32       0.0.0.0        0                    0       ?
```

查看 RouterB 发往 AS 10 的发布路由表时，可以看到表中没有 RouterB 发布的 AS 30 引入的直连路由。

```
<RouterB> display bgp routing-table peer 200.1.2.1 advertised-routes
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 2
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   200.1.2.0          200.1.2.2      0                    0       20?
 *>   200.1.3.0/24       200.1.2.2      0                    0       20?
```

同样，RouterA 的 BGP 路由表里也没有这些路由。

```
<RouterA> display bgp routing-table
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 8
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         0.0.0.0        0                    0       ?
 *>   9.1.1.1/32         0.0.0.0        0                    0       ?
 *>   127.0.0.0          0.0.0.0        0                    0       ?
 *>   127.0.0.1/32       0.0.0.0        0                    0       ?
 *>   200.1.2.0          0.0.0.0        0                    0       ?
 *                       200.1.2.2      0                    0       20?
 *>   200.1.2.1/32       0.0.0.0        0                    0       ?
 *>   200.1.3.0/24       200.1.2.2      0                    0       20?
```

15.3.6　接收和发布路由过滤的配置示例

本示例的基本拓扑结构如图 15-3 所示，在运行 OSPF 协议的网络中，RouterA 从 Internet 网络接收路由，并为 OSPF 网络提供了 Internet 路由。现要求 OSPF 网络只能访问 172.1.17.0/24、172.1.18.0/24 和 172.1.19.0/24 三个网段的网络，其中 RouterC 连接的网络只能访问 172.1.18.0/24 网段的网络。

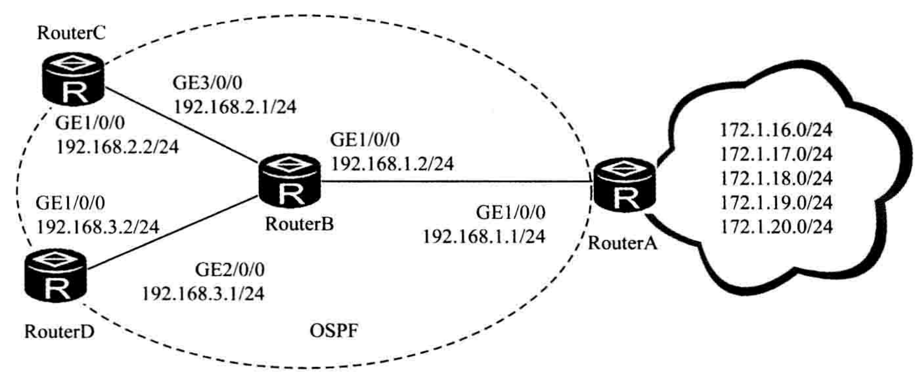


图 15-3 对接收和发布的路由过滤配置示例拓扑结构

1. 基本配置思路分析

本示例是利用 IP 地址列表过滤器对发布和接收的路由进行过滤，具体的配置思路如下。

① 在 RouterA 上配置过滤策略，使其在路由发布时仅提供 172.1.17.0/24、172.1.18.0/24、172.1.19.0/24 路由给 RouterB，使得 OSPF 网络只能访问 172.1.17.0/24、172.1.18.0/24 和 172.1.19.0/24 三个网段的网络。

② 在 RouterC 上配置过滤策略，使其在进行路由引入时仅接收 172.1.18.0/24 路由，使得 RouterC 连接的网络只能访问 172.1.18.0/24 网段的网络。

当然，首先还是要配置各路由器接口 IP 地址及 OSPF 网络中各路由的 OSPF 基本功能。

2. 具体配置步骤

① 配置各路由器的接口 IP 地址。以下是 RouterB 上接口 IP 地址的配置，其他路由器上接口 IP 地址的配置方法一样，略。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterB-GigabitEthernet1/0/0]quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 192.168.3.1 24
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] ip address 192.168.2.1 24
```

② 配置 OSPF 网络中各路由器的 OSPF 基本功能，使彼此三层互通。因为它们位于一个区域中，所以只能采用骨干区域 0 进行配置，进程号为缺省的 1。

RouterA 上的配置如下。

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

RouterB 上的配置如下。

```
[RouterB] ospf
[RouterB-ospf-1] area 0
```

```
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

RouterC 上的配置如下。

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

RouterD 上的配置如下。

```
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
```

③ 在 RouterA 上配置 5 条静态路由，并将这些静态路由引入 OSPF 协议中。这里的 5 条静态路由均为黑洞（出接口为 NULL0）静态路由。本示例这样配置仅为了实验。

```
[RouterA] ip route-static 172.1.16.0 24 NULL 0
[RouterA] ip route-static 172.1.17.0 24 NULL 0
[RouterA] ip route-static 172.1.18.0 24 NULL 0
[RouterA] ip route-static 172.1.19.0 24 NULL 0
[RouterA] ip route-static 172.1.20.0 24 NULL 0
[RouterA] ospf
[RouterA-ospf-1] import-route static
[RouterA-ospf-1] quit
```

此时可在 RouterB 上通过 **display ip routing-table** 命令查看其 IP 路由表，从输出信息中可以见到，OSPF 已成功引入了以上 5 条静态路由（**参见输出信息粗体字部分**）。

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    172.1.16.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.1.17.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.1.18.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.1.19.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.1.20.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
   192.168.1.0/24   Direct 0    0           D   192.168.1.2     GigabitEthernet1/0/0
   192.168.1.1/32   Direct 0    0           D   192.168.1.1     GigabitEthernet1/0/0
   192.168.1.2/32   Direct 0    0           D   127.0.0.1       InLoopBack0
   192.168.2.0/24   Direct 0    0           D   192.168.2.1     GigabitEthernet3/0/0
   192.168.2.1/32   Direct 0    0           D   127.0.0.1       InLoopBack0
   192.168.2.2/32   Direct 0    0           D   192.168.2.2     GigabitEthernet3/0/0
   192.168.3.0/24   Direct 0    0           D   192.168.3.1     GigabitEthernet2/0/0
   192.168.3.1/32   Direct 0    0           D   127.0.0.1       InLoopBack0
   192.168.3.2/32   Direct 0    0           D   192.168.3.2     GigabitEthernet2/0/0
```

④ 配置路由发布过滤策略。首先在 RouterA 上配置 IP 地址前缀列表 a2b，仅允许 172.1.17.0/24、172.1.18.0/24 和 172.1.19.0/24 三个网段的路由通过。

```
[RouterA] ip ip-prefix a2b index 10 permit 172.1.17.0 24
```

```
[RouterA] ip ip-prefix a2b index 20 permit 172.1.18.0 24
[RouterA] ip ip-prefix a2b index 30 permit 172.1.19.0 24
```

然后在 RouterA 上创建一个 IP 地址前缀列表过滤器，调用前面创建的 IP 地址前缀列表 a2b 对发布的静态路由进行过滤。

```
[RouterA] ospf
[RouterA-ospf-1] filter-policy ip-prefix a2b export static
```

此时在 RouterB 上可通过 **display ip routing-table** 命令再次查看其 IP 路由表，从中可以看到此时 RouterB 仅接收到列表 a2b 中定义的 3 条路由（**参见输出信息粗体字部分**）。

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.1.17.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.18.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.19.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.0/24  Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
    192.168.1.1/32  Direct  0    0           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet3/0/0
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.2.2/32  Direct  0    0           D   192.168.2.2     GigabitEthernet3/0/0
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet2/0/0
    192.168.3.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.3.2/32  Direct  0    0           D   192.168.3.2     GigabitEthernet2/0/0
```

⑤ 配置路由接收过滤策略。在 RouterC 上配置一个 IP 地址前缀列表 in，仅允许接收 172.1.18.0/24 的路由。

```
[RouterC] ip ip-prefix in index 10 permit 172.1.18.0 24
```

然后在 RouterC 上配置接收策略，引用地址前缀列表 in 进行过滤。

```
[RouterC] ospf
[RouterC-ospf-1] filter-policy ip-prefix in import
```

此时再在 RouterC 上通过 **display ip routing-table** 命令查看 IP 路由表，可以看到 RouterC 的本地核心路由表中，仅接收了列表 in 定义的 1 条路由（参见输出信息粗体字部分）。

```
[RouterC]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.1.18.0/24  O_ASE   150  1           D   192.168.2.1     GigabitEthernet1/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.2     GigabitEthernet1/0/0
    192.168.2.1/32  Direct  0    0           D   192.168.2.1     GigabitEthernet1/0/0
    192.168.2.2/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

而此时查看 RouterD 的 IP 路由表，可以看到 RouterD 的本地 IP 路由表中接收了 RouterB 发送的所有路由（**参见输出信息粗体字部分**）。

```
[RouterD] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10         Routes : 10

Destination/Mask    Proto    Pre   Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct   0     0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32   Direct   0     0           D   127.0.0.1       InLoopBack0
    172.1.17.0/24   O_ASE    150   1           D   192.168.3.1     GigabitEthernet1/0/0
    172.1.18.0/24   O_ASE    150   1           D   192.168.3.1     GigabitEthernet1/0/0
    172.1.19.0/24   O_ASE    150   1           D   192.168.3.1     GigabitEthernet1/0/0
   192.168.1.0/24   OSPF     10    1           D   192.168.3.1     GigabitEthernet1/0/0
   192.168.2.0/24   OSPF     10    1           D   192.168.3.1     GigabitEthernet1/0/0
   192.168.3.0/24   Direct   0     0           D   192.168.3.2     GigabitEthernet1/0/0
   192.168.3.1/32   Direct   0     0           D   192.168.3.1     GigabitEthernet1/0/0
   192.168.3.2/32   Direct   0     0           D   127.0.0.1       GigabitEthernet1/0/0
```

但通过 **display ospf routing** 命令查看 RouterC 的 OSPF 路由表时，可以看到 OSPF 路由表中仍然接收了 IP 地址列表 a2b3 中所定义的全部 3 条路由（**参见输出信息粗体字部分**）。因为 **filter-policy import** 命令用于过滤从协议路由表加入本地 IP 路由表的路由，不过滤加入协议路由表中的路由。

```
[RouterC] display ospf routing
          OSPF Process 1 with Router ID 192.168.2.2
                   Routing Tables

 Routing for Network
 Destination        Cost   Type       NextHop         AdvRouter       Area
 192.168.2.0/24     1      Stub       192.168.2.2     192.168.2.2     0.0.0.0
 192.168.1.0/24     2      Stub       192.168.2.1     192.168.2.1     0.0.0.0
 192.168.3.0/24     2      Stub       192.168.2.1     192.168.2.1     0.0.0.0

 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop          AdvRouter
 172.1.17.0/24      1         Type2      1           192.168.2.1      192.168.1.1
 172.1.18.0/24      1         Type2      1           192.168.2.1      192.168.1.1
 172.1.19.0/24      1         Type2      1           192.168.2.1      192.168.1.1

 Total Nets: 6
 Intra Area: 3    Inter Area: 0    ASE: 3    NSSA: 0
```

15.3.7 在路由引入时应用路由策略的配置示例

本示例的基本拓扑结构如图 15-4 所示，RouterB 与 RouterA 之间通过 OSPF 协议交换路由信息，与 RouterC 之间通过 IS-IS 协议交换路由信息。要求在 RouterB 上将 IS-IS 网络中路由引入 OSPF 网络，172.17.1.0/24 路由的选路优先级较低；172.17.2.0/24 路由具有标记，以便以后运用路由策略。

1．基本配置思路分析

本示例采用路由策略对引入的路由进行控制，基本配置思路如下。

① 在 RouterB 上配置路由策略，将 172.17.1.0/24 的路由的开销设置为 100（路由的

缺省开销值为 0），并在 OSPF 引入 IS-IS 路由时应用路由策略，使得 OSPF 网络中 172.17.1.0/24 路由的选路优先级较低；将 172.17.2.0/24 的路由的 Tag 属性设置为 20，使得路由 172.17.2.0/24 具有标识，方便下面应用路由策略。

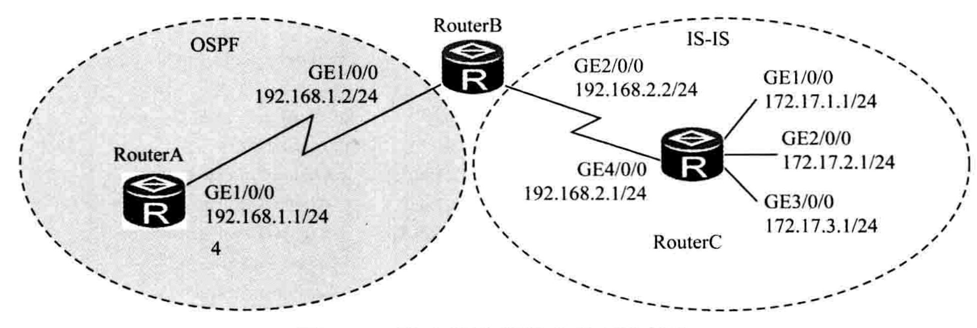


图 15-4 路由策略配置示例拓扑结构

② 在 RouterB 上配置路由策略，将 172.17.2.0/24 的路由的 Tag 属性设置为 20，并在 OSPF 引入 IS-IS 路由时应用路由策略，使得路由 172.17.2.0/24 具有标识，方便以后运用路由策略。

同样，首先还是要配置各路由器接口 IP 地址及 OSPF、IS-IS 网络中各路由的基本功能。

2. 具体配置步骤

① 配置各路由器的接口 IP 地址。以下是 RouterB 上接口 IP 地址的配置，其他路由器上接口 IP 地址的配置方法一样，略。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterB-GigabitEthernet1/0/0]quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 192.168.2.2 24
[RouterB-GigabitEthernet2/0/0] quit
```

② 在 RouterC 和 RouterB 上配置 IS-IS 协议基本功能，假设区域 ID 为 10，各自的 System ID 分别为 0000.0000.0001 和 0000.0000.0002。因为本示例中的 IS-IS 网络中只有一个区域，所以它们均只能作为骨干路由器，即 Level-2 路由器。

RouterC 上的配置如下。

```
[RouterC] isis
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity 10.0000.0000.0001.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 4/0/0
[RouterC-GigabitEthernet4/0/0] isis enable
[RouterC-GigabitEthernet4/0/0] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable
[RouterC-GigabitEthernet2/0/0] quit
```

```
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] isis enable
[RouterC-GigabitEthernet3/0/0] quit
```

RouterB 上的配置如下。

```
[RouterB] isis
[RouterB-isis-1] is-level level-2
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis enable
[RouterB-GigabitEthernet2/0/0] quit
```

③ 在 RouterA 和 RouterB 上配置 OSPF 协议基本功能，并配置 RouterB 引入 IS-IS 路由。同样，由于只有一个区域，所以只能采用骨干区域 0。

RouterA 上的配置如下。

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

RouterB 上的配置如下。

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] import-route isis 1
[RouterB-ospf-1] quit
```

此时可在 RouterA 上通过 display ospf routing 命令查看其 OSPF 路由表，从中可以看到由 RouterB 引入并通告的 IS-IS 路由（**参见输出信息中粗体字部分**）。

```
[RouterA] display ospf routing
          OSPF Process 1 with Router ID 192.168.1.1
                   Routing Tables
 Routing for Network
 Destination        Cost  Type        NextHop         AdvRouter       Area
 192.168.1.0/24     1   Stub        192.168.1.1     192.168.1.1     0.0.0.0
 Routing for ASEs
 Destination        Cost      Type        Tag         NextHop         AdvRouter
 172.17.1.0/24      1         Type2       1           192.168.1.2     192.168.1.2
 172.17.2.0/24      1         Type2       1           192.168.1.2     192.168.1.2
 172.17.3.0/24      1         Type2       1           192.168.1.2     192.168.1.2
 192.168.2.0/24     1         Type2       1           192.168.1.2     192.168.1.2
 Total Nets: 5
 Intra Area: 1   Inter Area: 0   ASE: 4   NSSA: 0
```

④ 在 RouterB 上配置基本 ACL（也可采用 IP 地址前缀列表）的过滤，仅允许 172.17.2.0/24 路由信息通过，用于下面在路由策略中为该路由配置路由标记。

```
[RouterB] acl number 2002
[RouterB-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
[RouterB-acl-basic-2002] quit
```

配置名为 prefix-a 的 IP 地址前缀列表（也可采用基本 ACL 过滤），仅允许 172.17.1.0/24 路由信息通过，用于路由策略中为该路由重新配置路由开销值。

```
[RouterB] ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
```

创建一条路由策略，并分别调用前面配置的 ACL 和 IP 地址前缀列表，为 172.17.2.0/24 路由信息打上标记号 20，为 172.17.1.0/24 路由信息设置路由开销值为 100，以降低它的优先级。

```
[RouterB] route-policy isis2ospf permit node 10
[RouterB-route-policy] if-match ip-prefix prefix-a
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] route-policy isis2ospf permit node 20
[RouterB-route-policy] if-match acl 2002
[RouterB-route-policy] apply tag 20
[RouterB-route-policy] quit
[RouterB] route-policy isis2ospf permit node 30
[RouterB-route-policy] quit
```

【经验之谈】在上面的配置中我们加了一个节点 30 的策略项，但其中并没有 **if-match** 和 **appy** 子句。节点 30 的策略项不是可有可无的。因为在路由策略中，是按照路由策略各节点从小到大依次进行匹配的，如果没有 30 这个节点策略，则凡是不与节点 10 和节点 20 的策略匹配的所引入的 IS-IS 路由都将被拒绝通过。这显然不与本示例的期望相符，所以必须要加上节点 30，直接让其他引入的 IS-IS 路由通过，但不作属性修改。

⑤ 配置 RouterB 在路由引入时应用前面创建的路由策略。

```
[RouterB] ospf
[RouterB-ospf-1] import-route isis 1 route-policy isis2ospf
[RouterB-ospf-1] quit
```

此时可在 RouterA 上通过命令查看其 OSPF 路由表，从中可以看到目的地址为 172.17.1.0/24 的路由的开销为 100，目的地址为 172.17.2.0/24 的路由的标记域（Tag）为 20，而其他路由的属性未发生变化（**参见输出信息中粗体字部分**）。符合本示例的要求，证明配置是成功的。

```
[RouterA] display ospf routing
          OSPF Process 1 with Router ID 192.168.1.1
                   Routing Tables
 Routing for Network
 Destination        Cost  Type       NextHop        AdvRouter      Area
 192.168.1.0/24     1     Stub       192.168.1.1    192.168.1.1    0.0.0.0
 Routing for ASEs
 Destination        Cost      Type       Tag        NextHop        AdvRouter
 172.17.1.0/24      100       Type2      1          192.168.1.2    192.168.1.2
 172.17.2.0/24      1         Type2      20         192.168.1.2    192.168.1.2
 172.17.3.0/24      1         Type2      1          192.168.1.2    192.168.1.2
 192.168.2.0/24     1         Type2      1          192.168.1.2    192.168.1.2
 Total Nets: 5
 Intra Area: 1   Inter Area: 0   ASE: 4   NSSA: 0
```

15.4 策略路由基础

本章前面介绍了“路由策略”（Routing Policy，RP），它与本节将要介绍的“策略路由”（Policy-Based Routing，PBR）看似是两个词位置的互换，但却有着本质上的区别。“路由策略”中的“路由”是名词，而“策略”是动词，**操作对象是路由信息**。“路由策略”**主要**

用来实现路由表中的路由过滤和路由属性设置等功能。它通过改变路由属性（包括可达性）来改变网络流量所经过的路径。而“策略路由”中的“策略”是名词，“路由”却变成了动词，是基于策略的路由（这里的“路由”也是动词），**操作对象是数据报文**，是在路由表已经产生的情况下，不按照路由表进行转发，而是根据需要按照某种策略改变数据报文转发路径。

15.4.1 策略路由概述

传统的路由转发原理是首先根据报文的目的地址查找路由表，然后进行报文转发。但是目前越来越多的用户希望能够在传统路由转发的基础上根据自己定义的策略进行报文转发和选路。策略路由正是这样一种可依据用户制定的策略进行报文路由选路的机制。策略路由可使网络管理者不仅能够根据报文的目的地址，而且能够根据报文的源地址、报文大小和链路质量等属性来制定策略路由，以改变报文转发路径，满足用户需求。

策略路由具有如下优点。

① 可以根据用户实际需求制定策略进行路由选择，增强路由选择的灵活性和可控性。

② 可以使不同的数据流通过不同的链路进行发送，提高链路的利用效率。

③ 在满足业务服务质量的前提下，选择费用较低的链路传输业务数据，从而降低企业数据服务的成本。

总体来说，“路由策略”和“策略路由”的区别如表 15-5 所示。

表 15-5　路由策略与策略路由的区别

区别项目	路由策略	策略路由
作用对象	作用对象是路由信息	作用对象是数据流
转发规则	按路由表转发	基于策略的转发，失败后再查找路由表转发
服务对象	基于控制平面，为路由协议和路由表服务	基于转发平面，为转发策略服务
实现方式	与路由协议结合完成策略	需要手工逐跳配置，以保证报文按策略转发

华为 AR G3 系列路由器支持以下三种策略路由：本地策略路由、接口策略路由和智能策略路由（Smart Policy Routing，SPR），如表 15-6 所示。设备配置策略路由后，当设备下发或转发数据报文时，系统首先根据策略路由转发，若没有配置策略路由或配置了策略路由但找不到匹配的表项时，再根据路由表来转发。

表 15-6　三种策略路由

策略路由类别	功能	应用场景
本地策略路由	**对本设备发送的报文**实现策略路由，比如本机下发的 ICMP、BGP 等协议报文	当用户需要使不同源地址报文或者不同长度的报文通过不同的方式进行发送时，可以配置本地策略路由
接口策略路由	**对本设备转发的报文**实现策略路由，对本机下发的报文不生效	当用户需要将到达接口的某些报文通过特定的下一跳地址进行转发时，需要配置接口策略路由。使匹配重定向规则的转发报文通过特定的下一跳出口进行转发，不匹配重定向规则的转发报文根据路由表转发。接口策略路由多应用于负载分担和安全监控
智能策略路由	**基于链路质量信息**为业务数据流选择最佳链路	当用户需要为不同业务选择不同质量的链路时，可以配置智能策略路由

说明 缺省情况下，设备的 SPR 功能受限无法使用，需要使用 License 授权。如果需要使用 SPR 功能，请联系华为办事处申请并购买对应系列的数据业务增值包。

15.4.2 本地策略路由

“本地策略路由”是**仅对本机发送的报文**（比如本地的 Ping 报文）**有效的策略路由，对转发的报文不起作用。**

一条本地策略路由可以配置多个策略点，并且这些策略点具有不同的优先级，本机发送的报文优先匹配优先级高的策略点。本地策略路由支持基于 ACL 或报文长度的匹配规则。

在本地策略路由中，当本机下发报文时，会根据本地策略路由节点的优先级，依次匹配各节点绑定的匹配规则。如果找到了匹配的本地策略路由节点，则按照以下步骤发送报文；如果没有找到匹配的本地策略路由节点，按照发送 IP 报文的一般流程，根据目的地址查找路由。

（1）查看用户是否设置了报文的优先级

如果用户设置了报文的优先级，则首先根据用户设置的优先级设置报文的优先级，然后继续执行下一步；否则直接进行下一步。由此可以看出，报文的优先级是首先要考虑的规则。

（2）查看用户是否设置了本地策略路由的出接口

如果用户设置了出接口，将报文从出接口发送出去，不再执行下面步骤；否则直接进行下一步。

（3）查看用户是否设置了本地策略路由的下一跳

① 如果设置了策略路由的下一跳，且下一跳可达，则查看是否设置了下一跳联动路由。

a. 如果设置了下一跳联动路由功能，设备会根据配置的联动路由的 IP 地址检测该 IP 地址是否路由可达。

- 如果该 IP 地址路由可达，则配置的下一跳生效，设备将报文发往下一跳，不再执行下面步骤。

- 如果该 IP 地址路由不可达，则配置的下一跳不生效，设备会继续查看是否配置备份下一跳。

  ➢ 如果用户配置了备份下一跳，且备份下一跳可达，将报文发往备份下一跳，不再执行下面的步骤。

  ➢ 如果用户未配置备份下一跳，或配置的备份下一跳不可达，则按照正常流程根据报文的目的地址查找路由。如果没有查找到路由，则执行下一步。

b. 如果用户未设置下一跳联动路由功能，将报文发往下一跳，不再执行下面的步骤。

② 如果设置了策略路由的下一跳，但下一跳不可达，则设备会继续查看是否配置备份下一跳。

a. 如果用户配置了备份下一跳，且备份下一跳可达，将报文发往备份下一跳，不再

执行下面的步骤。

b. 如果用户未配置备份下一跳，或配置的备份下一跳不可达，则按照正常流程根据报文的目的地址查找路由。如果没有查找到路由，则执行下一步。

③ 如果用户未设置下一跳，则按照正常流程根据报文的目的地址查找路由。如果没有查找到路由，则执行下一步。

（4）查看用户是否设置了本地策略路由的缺省出接口

① 如果用户设置了缺省出接口，将报文从缺省出接口发送出去，不再执行下面的步骤。

② 如果用户未设置缺省出接口，则执行下一步。

（5）查看用户是否设置了本地策略路由的缺省下一跳

① 如果用户设置了缺省下一跳，将报文发往缺省下一跳，不再执行下面的步骤。

② 如果用户未设置缺省下一跳，则执行下一步

（6）丢弃报文，产生 ICMP_UNREACH 消息

15.4.3　接口策略路由

“接口策略路由”与前面介绍的“本地策略路由”相反，**它仅对转发的报文起作用，对本地发送的报文不起作用，且只对接口入方向的报文生效。**

接口策略路由是通过在流行为中配置重定向实现的。缺省情况下，设备按照路由表的下一跳进行报文转发，如果配置了接口策略路由，则设备按照接口策略路由指定的下一跳进行转发。

在按照接口策略路由指定的下一跳进行报文转发时，如果设备上没有该下一跳 IP 地址对应的 ARP 表项，设备会触发 ARP 学习。如果设备上有，或者学习到了此 ARP 表项，则按照接口策略路由指定的下一跳 IP 地址进行报文转发；如果一直学习不到下一跳 IP 地址对应的 ARP 表项，则报文按照路由表指定的下一跳进行转发。

15.4.4　智能策略路由

随着网络业务需求的多样化，业务数据的集中放置，链路质量对网络业务越来越重要。越来越多的用户把关注点从网络的连通性转移到业务的可用性上，如业务的可获得性、响应速度和业务质量等。这些复杂的业务需求给传统的基于逐跳的路由协议提出了挑战，它们无法感知链路的质量和业务的需求，所以带给用户的业务体验也得不到保障，即使路由可达，但链路质量可能已经很差甚至无法正常转发报文了。

智能策略路由 SPR 就是在这一背景下产生的一种策略路由。它可以主动探测链路质量并匹配业务的需求，通过匹配链路质量和网络业务对链路质量的需求，从而选择一条最优链路转发业务数据，可以有效地避免网络黑洞、网络振荡等问题。因为相对来说，这种策略路由的应用比较少，故本章仅介绍其基础知识，不介绍其具体的配置方法。

1. 业务区分

SPR 支持通过以下属性对业务进行区分。

① 根据协议类型区分：IP，TCP，UDP，GRE，IGMP，IPINIP，OSPF，ICMP。

② 根据报文应用区分：DSCP（区分服务代码点），TOS（服务类型），IP Precedence（IP 优先级），Fragment（分片），VPN，TCP-flag（TCP 标志）。

③ 根据报文信息区分：Source IP Address（源 IP 地址），Destination IP Address（目的 IP 地址），Protocol（协议），Source Port（源端口），Destination Port（目的端口），Source IP Prefix（源 IP 地址前缀），Destination IP Prefix（目的 IP 地址前缀）。

不同的业务对链路的时延 D（Delay）、抖动时间 J（Jitter）、丢包率 L（Loss）以及 CMI（Composite Measure Indicator，综合度量指标）有不同的要求，如果业务对链路的某一项质量参数没有要求，就不需要配置该参数的阈值。具体将在后面介绍 SPR 配置时介绍。

2. 探测链路和链路组

探测链路是 SPR 实现智能选路的基础，每个探测链路都有一个与之相对应的探针，即 NQA（Network Quality Analysis，网络质量分析）测试例。如果测试失败，则表示对应的探测链路不可用。探测链路通过探针获取链路参数的质量，SPR 根据探测链路的链路质量匹配业务需求，从而实现智能选路的需求。

SPR 的链路角色分为主用链路组、备用链路组和逃生链路。当在 SPR 中业务无法从主用链路组和备用链路组中找到合适的链路传输数据时可以启用逃生链路。SPR 根据 NQA 探测结果进行业务选路的具体流程如图 15-5 所示。

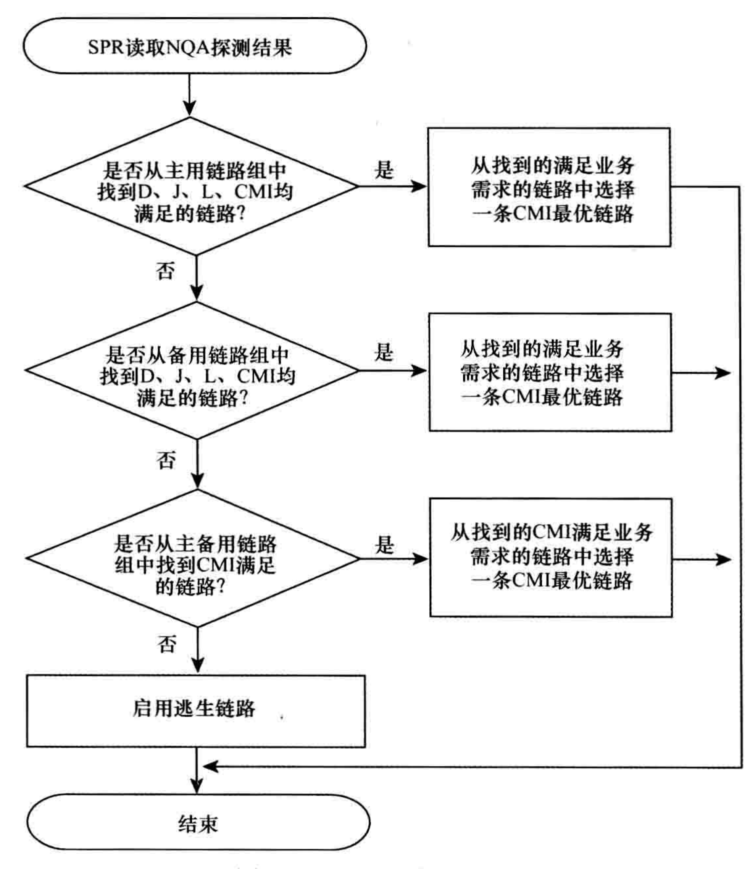


图 15-5 SPR 业务选路流程

SPR 不直接使用探测链路，而是通过链路组的形式使用探测链路。一个探测链路可以加入不同的链路组，同时一个链路组中可以有一条或多条探测链路。同一个链路组可以被不同的业务绑定，如链路组 1 可以作为业务 1 的主用链路组，同时也可以作为业务 2 的备用链路组。

在业务选路时，如果当前链路上已经部属了业务，则该链路的选择指数将降低，即选择的机率变小，这样宏观上可以达到负载均衡的效果。

3. 切换周期

SPR 中的切换周期计时器主要用于在链路质量不满足业务需求时控制链路切换。

SPR 根据 NQA 探测结果判断链路是否满足业务需求，SPR 会定期获取 NQA 的探测结果，如果某次获取的 NQA 探测结果不满足业务需求，则切换周期计时器开始计时。在开始计时后到切换周期到达之前，如果某次获取的探测结果满足了业务需求，则切换周期计时器清零，直到下次获取到不满足业务需求的探测结果时会再次开始计时。如果计时器开始计时后，在切换周期内获取到的探测结果都不能满足业务需求，则 SPR 切换链路。

4. 振荡抑制周期

某些情况下，网络会出现时好时坏的情况，从而导致 SPR 频繁切换链路，这样会严重影响业务体验。SPR 的抑制振荡功能可以有效地避免此类情况产生。但振荡抑制周期默认情况下不生效，周期值由用户自己配置。

SPR 切换链路后，振荡抑制周期计时器开始计时，如果业务驻留链路的时间没有达到振荡抑制周期的时间，则 SPR 不会执行链路切换。振荡抑制周期超时后，如果在一个切换周期内链路还是不满足业务需求，则 SPR 将切换链路；如果在一个切换周期内链路质量变好，满足业务需求，则 SPR 不会切换链路。

15.5　本地策略路由配置与管理

通过配置本地策略路由，可以控制直接由本机发送的报文通过指定的出接口进行发送。也就是，本地策略路由只对主机面下发的数据生效。

本地策略路由配置思路是，先配置用于数据报文匹配的本地策略路由的匹配规则，然后配置本地策略路由的动作，最后在出接口上应用以上配置的本地策略路由。由此可见，本地策略路由包括以下三项主要配置任务（**要按顺序配置**）。

① 创建一个本地策略路由。

② 通过 **apply** 命令配置本地策略路由的动作。

③ 在系统视图下全局应用前面创建本地策略路由。

但在配置本地策略路由之前，需完成以下任务。

- 配置接口的链路层协议参数，使接口的链路协议状态为 Up。
- 配置用于匹配报文的 ACL。这里就**不仅限于基本 ACL**，还可以用高级 ACL 同时过滤报文的源 IP 地址、目的 IP 地址、源端口、目的端口等。
- 如果希望报文进入 VPN，则需要预先配置 VPN。

15.5.1 配置本地策略路由的匹配规则

本地策略路由的匹配规则就是用来定义要通过本地策略路由进行过滤的报文，通过ACL或者匹配报文长度（**可单独配置，也可同时配置**）进行过滤的，具体配置步骤如表15-7所示。

表15-7 本地策略路由的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**policy-based-route** *policy-name* { **deny** | **permit** } **node** *node-id* 例如：[Huawei] **policy-based-route** pbr1 **permit node** 10	创建策略路由和策略点，若策略点已创建则进入本地策略路由视图。命令中的参数说明如下 ● *policy-name*：指定要创建的策略名称，1～19个字符，不支持空格，区分大小写 ● **deny**：二选一选项，设置策略点的匹配模式为拒绝模式，表示对满足匹配条件的报文不进行策略路由 ● **permit**：二选一选项，设置策略点的匹配模式为允许模式，表示对满足匹配条件的报文进行策略路由 ● *node node-id*：指定策略点的顺序号，取值范围为0～65 535的整数。策略点顺序号的值越小则优先级越高，相应策略优先执行 重复执行本命令可以在一条本地策略路由下创建多个策略点 缺省情况下，本地策略路由中未创建策略路由或策略点，可用undo policy-based-route policy-name [permit | deny | node node-id]命令删除本地策略路由中指定的策略路由或策略点
3	**if-match acl** *acl-number* 例如：[Huawei-policy-based-route-policy1-10] **if-match acl 2000**	（可选）设置本地策略路由中IP报文的ACL匹配条件。参数*acl-number*用来指定要调用的ACL号，取值范围是2 000～3 999的整数，其中2 000～2 999是基本访问控制列表，3 000～3 999是高级访问控制列表。**但该ACL必须事先配置好。它与下面的报文长度过滤可以单独配置，也可以同时配置** 【注意】因为在策略的执行过程中有本地策略路由和ACL两处匹配模式，所以在配置时要注意以下的匹配结果 ● 当ACL的rule配置为**permit**时，设备会对匹配该规则的报文执行本地策略路由相应的动作：如果本地策略路由中策略点为**permit**，则对通过ACL匹配条件的报文进行策略路由；如果本地策略路由中策略点为**deny**，则对通过ACL匹配条件的报文不进行策略路由，仍根据目的地址查找路由表转发报文 ● 当ACL配置了rule，但报文未匹配上ACL加的任何规则，则该报文仍根据目的地址查找路由表转发报文 ● 当ACL的rule配置为**deny**或ACL未配置规则时，应用该ACL的本地策略路由不生效，即根据目的地址查找路由表转发报文 另外，如果在策略路由的同一个策略点下多次配置了本命令，则按最后一次配置结果生效 缺省情况下，本地策略路由中未配置IP地址匹配条件，可用**undo if-match acl**命令删除本地策略路由中的IP地址匹配条件

（续表）

步骤	命令	说明
4	**if-match packet-length** *min-length max-length* 例如：[Huawei-policy-based-route-map1-10] **if-match packet-length** 100 200	（可选）设置 IP 报文长度匹配条件。**它与上面的 ACL 过滤可以单独配置，也可以同时配置**。命令中的参数说明如下 ● *min-length*：指定策略路由要匹配的最短 IP 报文长度，取值范围为 0～65 535 整数个字节 ● *max-length*：指定策略路由要匹配的最长 IP 报文长度，取值范围为 1～65 535 整数个字节，且不能小于 *min-length* 参数值 在策略路由的同一个策略节点下多次执行该命令，按最后一次配置结果生效 缺省情况下，本地策略路由中未配置 IP 报文长度匹配条件，可用 **undo if-match packet-length** 命令删除本地策略路由中 IP 报文长度匹配条件的配置

15.5.2　配置本地策略路由的动作

配置本地策略路由的动作是指对通过本地策略路由的报文进行出接口、下一跳（相当于对流进行重定向），或者 IP 报文优先级指定等。配置时要注意以下情形。

① 如果策略中设置了两个下一跳，那么报文转发在两个下一跳之间负载分担。

② 如果策略中设置了两个出接口，那么报文转发在两个出接口之间负载分担。

③ 如果策略中同时设置了两个下一跳和两个出接口，那么报文转发仅在两个出接口之间负载分担。

本地策略路由的动作配置步骤如表 15-8 所示。

表 15-8　　本地策略路由的动作配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**policy-based-route** *policy-name* { **deny** | **permit** } **node** *node-id* 例如：[Huawei] **policy-based-route** pbr1 **permit node** 10	进入本地策略路由视图，其他说明参见上节表 15-7 中的第 2 步
以下命令是并列关系，没有先后次序，且均为可选配置，但一个策略点中至少包含下面一条 **apply** 子句，也可以多条 **apply** 子句组合使用		
3	**apply output-interface** *interface-type interface-number* 例如：[Huawei-policy-based-route-policy1-10]**apply output-interface** gigabitethernet 1/0/0	（可选）指定本地策略路由中报文的出接口。配置成功后，将匹配策略点的本机下发报文从指定出接口发送出去 缺省情况下，本地策略路由中未配置报文出接口，可用 **undo apply output-interface** *interface-type interface-number* 命令删除本地策略路由中指定的报文出接口配置 【注意】**报文的出接口不能为以太接口等广播型接口**，如是以太网接口要先用 **link-protocol ppp** 命令配置为 P2P 类型的，因为广播类型的接口有多个可能的下一跳，可能会造成报文转发不成功的现象 如果先使用本命令配置了两个出接口，然后又执行该命令配置了一个新的出接口，则后面配置的新出接口将覆盖前面配置的第一个出接口，而第二个出接口不会被覆盖

（续表）

步骤	命令	说明
3	**apply ip-address next-hop** *ip-address1* [*ip-address2*] 例如：[Huawei-policy-based-route-policy1-10]**apply ip-address next-hop** 1.1.1.1	（可选）设置本地策略路由中报文的下一跳。当该策略点未配置出接口时，匹配策略点的本机下发报文被发往指定的下一跳。命令中的参数说明如下 ● *ip-address1*：指定策略路由的下一跳 IP 地址，不能是本设备的 IP 地址 ● *ip-address2*：可选参数，指定策略路由的第二个下一跳 IP 地址，不能是本设备的 IP 地址。可以配置两个下一跳 IP 地址以达到负载分担的目的 缺省情况下，本地策略路由中未配置报文转发的下一跳，可用 undo apply ip-address next-hop [ip-address1] [ip-address2]命令删除本地策略路由中指定的报文转发下一跳配置 【注意】如果先使用本命令配置了两个下一跳，然后又执行该命令配置了一个新的下一跳，则新配置的下一跳将覆盖前面配置的第一个下一跳，而第二个下一跳不会被覆盖
	apply default output-interface *interface-type interface-number* 例如：[Huawei-policy-based-route-policy1-10] **apply default output-interface** gigabitethernet 1/0/10	（可选）配置本地策略路由中报文的缺省出接口，**同样不能为广播类型接口** 【说明】当该策略点未指定报文的出接口和下一跳，且匹配策略点的本机下发报文也未能按照正常流程根据报文目的地址查找到路由时，则将此报文从缺省出接口发送出去。由此可见，它只是一个最终的备份选择，如果已在本地策略中配置了出接口、下一跳，或者路由表中有对应的具体路由表项，则本命令的配置不生效 缺省情况下，本地策略路由中未配置报文的缺省出接口，可用 **undo apply default output-interface** [*interface-type interface-number*] 命令删除本地策略路由中指定的报文缺省出接口的配置
	apply ip-address default next-hop *ip-address1* [*ip-address2*] 例如：[Huawei-policy-based-route-policy1-10] **apply ip-address default next-hop** 1.1.1.10	（可选）配置本地策略路由中报文的缺省下一跳，**仅对在路由表中未查询到路由的报文起作用**。命令中的参数同前面介绍的 **apply ip-address next-hop** *ip-address1* [*ip-address2*] 命令中的对应参数。**报文的缺省下一跳地址也不能是本设备的 IP 地址** 缺省情况下，本地策略路由中未配置报文的缺省下一跳，可用 **undo apply ip-address default next-hop** [*ip-address1*] [*ip-address2*] 命令删除本地策略路由中指定的报文缺省下一跳的配置
	apply access-vpn vpn-instance *vpn-instance-name* &<1-6> 例如：[Huawei-policy-based-route-policy1-10] **apply access-vpn vpn-instance** vpn1 vpn2	（可选）设置本地策略路由中报文转发的 VPN 实例。当用户希望报文进入 VPN 时，可以执行本命令配置报文转发的 VPN 实例（但必须先创建对应的 VPN 实例），参数用来指定要进入的 VPN 实例的名称，1～31 个字符，不支持空格，区分大小写。在同一条命令中最多可以指定 6 个 VPN 实例名称 缺省情况下，本地策略路由中未配置报文转发的 VPN 实例，可用 **undo apply access-vpn vpn-instance** *vpn-instance-name* &<1-6>命令删除已配置的本地策略路由中报文转发的 VPN 实例

（续表）

步骤	命令	说明
3	**apply ip-precedence** *precedence* 例如：[Huawei-policy-based-route-policy1-10] **apply ip-precedence critical**	（可选）设置本地策略路由中IP报文优先级，取值范围为0～7的整数，值越大优先级越高，也可以使用优先级关键字代替优先级取值，两者的对应关系如表15-9所示。配置成功后，根据用户设置的报文优先级来设置匹配策略点的本机下发报文的优先级 缺省情况下，本地策略路由中未配置IP报文优先级，可用 **undo apply ip-precedence** 命令删除本地策略路由中IP报文优先级的配置
4	**quit** 例如：[Huawei-policy-based-route-policy1-10] **quit**	退出策略路由视图，返回系统视图
5	**ip policy-based-route refresh-time** *refreshtime-value* 例如：[Huawei] **ip policy-based-route refresh-time** 4000	（可选）配置本地策略路由刷新LSP信息的时间间隔，调整策略路由的执行效率。参数 *refreshtime-value* 用来指定策略路由定时器的时间间隔，取值范围为 1 000～65 535 的整数 ms 缺省情况下，本地策略路由刷新 LSP 信息的时间间隔为 5 000 ms，可用 **undo ip policy-based-route refresh-time** *refreshtime-value* 命令恢复本地策略路由刷新LSP信息的时间间隔为缺省值

IP 优先级取值与优先级关键字的对应关系如表 15-9 所示。

表 15-9　　IP 优先级取值与优先级关键字的对应关系

优先级取值	优先级关键字
0	Routine（普通）
1	Priority（优先）
2	Immediate（快速）
3	Flash（闪速）
4	Flash-override（疾速）
5	Critical（关键）
6	Internet（网间）
7	Network（网内）

15.5.3　应用本地策略路由

上面两节其实都可以看成是本地策略路由的配置过程，本节要介绍如何在本地设备上应用配置的本地策略路由的方法。

应用本地策略路由的方法很简单，只需在系统视图下通过 **ip local policy-based-route** *policy-name* 命令使能这条本地策略路由即可。这样在本机上直接发送的报文（不包括转发的报文）都将应用所使能的本地路由策略。但要注意，**一台路由器只能使能一个本地策略路由**（但可以创建多条本地策略路由），且本命令为覆盖式命令，多次执行该命令后，仅最后一次配置结果生效。**要使能其他本地策略路由时，必须先去使能正在应用的另一条本地策略路由。**

缺省情况下，所配置的本地策略路由处于未使能状态，可用 **undo ip local policy-based-route** [*policy-name*]命令去使能已使能的指定本地策略路由。

15.5.4 本地策略路由管理

创建并应用本地策略路由后，可通过以下任意视图命令查看相关信息，验证配置结果。

① **display ip policy-based-route**：看本地已使能的策略路由的策略。

② **display ip policy-based-route setup local** [**verbose**]：看本地策略路由的配置情况。

③ **display ip policy-based-route statistics local**：看本地策略路由报文的统计信息。

④ **display policy-based-route** [*policy-name* [**verbose**]]：看已创建的策略内容。

15.5.5 本地策略路由配置示例

本示例的基本拓扑结构如图 15-6 所示，RouterA 与 RouterB 间有两条链路相连。用户希望实现 RouterA 在发送不同长度的报文时通过不同的下一跳地址进行转发。

① 长度为 64～1 400 字节的报文设置 150.1.1.2 作为下一跳地址。

② 长度为 1 401～1 500 字节的报文设置 151.1.1.2 作为下一跳地址。

③ 所有其他长度的报文都按基于目的地址的方法进行路由选路。

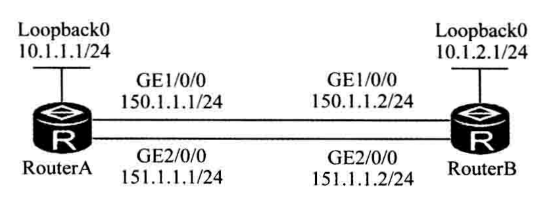


图 15-6 本地策略路由配置示例拓扑结构

1. 基本配置思路分析

本示例的要求很简单，仅需要通过在 RouterA 上配置一条匹配报文长度的本地策略路由，然后在 RouterA 上使能这条本地策略路由即可。但要注意的是，这里有两个不同的报文长度匹配规则，即 64～1 400 字节和 1 401～1 500 字节，所以需要配置两个不同的本地策略路由的策略点。

当然，在配置本地策略路由前，首先也得先配置这两台路由器上的各接口 IP 地址，为了使双方能与对方的 Loopback 接口所有网络互通（使报文长度不在 64～1 400 字节，或者 1 401～1 500 字节范围内的报文能够按照路由中配置的下一跳进行转发），还需要配置路由，本示例采用最简单的静态路由。

2. 具体配置步骤

① 按照图中标注配置两路由器上各接口的 IP 地址。

RouterA 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 150.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 151.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
```

```
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 10.1.1.1 255.255.255.0
[RouterA-LoopBack0] quit
```

RouterB 上的配置如下。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 150.1.1.2 255.255.255.0
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 151.1.1.2 255.255.255.0
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 10.1.2.1 255.255.255.0
[RouterB-LoopBack0] quit
```

② 配置 RouterA 和 RouterB 到达对方 Loopback 接口所在网络的静态路由。

```
[RouterA] ip route-static 10.1.2.0 24 150.1.1.2
[RouterA] ip route-static 10.1.2.0 24 151.1.1.2

[RouterB] ip route-static 10.1.1.0 24 150.1.1.1
[RouterB] ip route-static 10.1.1.0 24 151.1.1.1
```

③ 在 RouterA 上创建名称为 lab1 的本地策略路由，用策略点 10 和策略点 20 分别配置两种报文长度匹配规则，并分别指定对应策略点的动作，即指定对应的下一跳地址。

```
[RouterA] policy-based-route lab1 permit node 10
[RouterA-policy-based-route-lab1-10] if-match packet-length 64 1400
[RouterA-policy-based-route-lab1-10] apply ip-address next-hop 150.1.1.2
[RouterA-policy-based-route-lab1-10] quit
[RouterA] policy-based-route lab1 permit node 20
[RouterA-policy-based-route-lab1-20] if-match packet-length 1401 1500
[RouterA-policy-based-route-lab1-20] apply ip-address next-hop 151.1.1.2
[RouterA-policy-based-route-lab1-20] quit
```

在 RouterA 上使能以上本地策略路由 lab1。

```
[RouterA] ip local policy-based-route lab1
```

现在来验证配置结果。先在用户视图下使用 **reset counters interface** 命令清空 RouterB 上两个接口的报文数统计信息，以便能更好地验证后面的报文统计信息。此时两个接口上的各种报文统计均为 0。

```
<RouterB> reset counters interface gigabitethernet 1/0/0
<RouterB> reset counters interface gigabitethernet 2/0/0
```

在 RouterA 上 Ping RouterB 的 Loopback0，并将报文数据字段长度设为 80 字节（发送了 5 个 ICMP 报文，最终也显示接收了 5 个报文，**参见输出信息中的粗体字部分**）。

```
<RouterA> ping -s 80 10.1.2.1
  PING 10.1.2.1: 80    data bytes, press CTRL_C to break
    Reply from 10.1.2.1: bytes=80 Sequence=1 ttl=255 time=2 ms
    Reply from 10.1.2.1: bytes=80 Sequence=2 ttl=255 time=2 ms
    Reply from 10.1.2.1: bytes=80 Sequence=3 ttl=255 time=2 ms
    Reply from 10.1.2.1: bytes=80 Sequence=4 ttl=255 time=2 ms
    Reply from 10.1.2.1: bytes=80 Sequence=5 ttl=255 time=2 ms

  --- 10.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 2/2/2 ms
```

根据所配置的本地策略由，我们可以知道，这个长度的报文应该选择的是 RouterB 的 GE1/0/0 接口。此时查看 RouterB 接口统计信息，可以发现 GigabitEthernet 1/0/0 接收和发送报文总数都增加了 5（**参见输出信息中的粗体字部分**），即 RouterB 接口 GigabitEthernet 1/0/0 在接收到 ICMP 请求报文后给 RouterA 发送 5 个 ICMP 应答报文。证明配置是正确并成功的。

```
<RouterB> display interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-07-30 11:23:24
Description:HUAWEI, AR Series, GigabitEthernet1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 150.1.1.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0819-a6ce-7d4c
Last physical up time     : 2012-07-30 11:23:24
Last physical down time : 2012-07-24 16:54:19
Current system time: 2012-07-30 15:00:15
Port Mode: COMMON COPPER
Speed : 1000,   Loopback: NONE
Duplex: FULL,   Negotiation: ENABLE
Mdi     : AUTO
Last 300 seconds input rate 152 bits/sec, 0 packets/sec
Last 300 seconds output rate 16 bits/sec, 0 packets/sec
Input peak rate 7568 bits/sec,Record time: 2012-07-30 12:57:02
Output peak rate 1008 bits/sec,Record time: 2012-07-30 12:42:42

Input:   5 packets, 400 bytes
  Unicast:                      0,  Multicast:                0
  Broadcast:                    0,  Jumbo:                    0
  Discard:                      0,  Total Error:              0

  CRC:                          0,  Giants:                   0
  Jabbers:                      0,  Throttles:                0
  Runts:                        0,  Alignments:               0
  Symbols:                      0,  Ignoreds:                 0
  Frames:                       0

Output:   5 packets, 630 bytes
  Unicast:                      0,  Multicast:                0
  Broadcast:                    0,  Jumbo:                    0
  Discard:                      0,  Total Error:              0

  Collisions:                   0,  ExcessiveCollisions:      0
  Late Collisions:              0,  Deferreds:                0
  Buffers Purged:               0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization     : 0.00%
    Output bandwidth utilization : 0.00%
```

再次按照前面介绍的方法使用 **reset counters interface** 用户视图命令清空 RouterB 接

口统计信息。然后在 RouterA 上 Ping RouterB 的 Loopback0，并将报文数据字段长度设为 1 401 字节（也发送了 5 个 ICMP 报文，最终也显示接收了 5 个报文，**参见输出信息中的粗体字部分**）。

```
<RouterA> ping -s 1401 10.1.2.1
  PING 10.1.2.1: 1401   data bytes, press CTRL_C to break
    Reply from 10.1.2.1: bytes=1401 Sequence=1 ttl=255 time=1 ms
    Reply from 10.1.2.1: bytes=1401 Sequence=2 ttl=255 time=1 ms
    Reply from 10.1.2.1: bytes=1401 Sequence=3 ttl=255 time=1 ms
    Reply from 10.1.2.1: bytes=1401 Sequence=4 ttl=255 time=1 ms
    Reply from 10.1.2.1: bytes=1401 Sequence=5 ttl=255 time=2 ms

  --- 10.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

根据所配置的本地策略由，我们可以知道，这个长度的报文应该选择的是 RouterB 的 GE2/0/0 接口。此时查看 RouterB 接口统计信息，可以发现 GigabitEthernet 2/0/0 接收和发送报文总数都增加了 5（**参见输出信息中的粗体字部分**），即 RouterB 接口 GigabitEthernet 2/0/0 在接收到 ICMP 请求报文后给 RouterA 发送 5 个 ICMP 应答报文。证明配置是正确并成功的。

```
<RouterB> display interface gigabitethernet 2/0/0
GigabitEthernet2/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-07-30 11:23:29
Description:HUAWEI, AR Series, GigabitEthernet2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 151.1.1.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0819-a6ce-7d4d
Last physical up time     : 2012-07-30 11:23:29
Last physical down time : 2012-07-30 11:09:17
Current system time: 2012-07-30 16:04:55
Port Mode: COMMON COPPER
Speed : 1000,    Loopback: NONE
Duplex: FULL,    Negotiation: ENABLE
Mdi      : AUTO
Last 300 seconds input rate 200 bits/sec, 0 packets/sec
Last 300 seconds output rate 192 bits/sec, 0 packets/sec
Input peak rate 11576 bits/sec,Record time: 2012-07-30 13:46:52
Output peak rate 11576 bits/sec,Record time: 2012-07-30 13:46:52

Input:    6 packets, 7722 bytes
  Unicast:                  0,  Multicast:                0
  Broadcast:                0,  Jumbo:                    0
  Discard:                  0,  Total Error:              0

  CRC:                      0,  Giants:                   0
  Jabbers:                  0,  Throttles:                0
  Runts:                    0,  Alignments:               0
  Symbols:                  0,  Ignoreds:                 0
  Frames:                   0
```

```
Output:  5 packets, 7235 bytes
  Unicast:                      0,  Multicast:                 0
  Broadcast:                    0,  Jumbo:                     0
  Discard:                      0,  Total Error:               0

  Collisions:                   0,  ExcessiveCollisions:       0
  Late Collisions:              0,  Deferreds:                 0
  Buffers Purged:               0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization   : 0.00%
    Output bandwidth utilization : 0.00%
```

说明 在以上输出信息中，之所以接收的报文数不是5个，而是6个，原因是该接口可能在我们进行统计前又接受了其他类型的报文。这里只需要从总体上验证不同长度的报文是否按照策略路由的配置选择了不同的下一跳，而不需要证明对应接口只能接受我们进行测试的ICMP报文。

15.6 接口策略路由配置与管理

配置接口策略路由可以将到达接口**转发的报文**（不对本机直接发送的报文生效）重定向到指定的下一跳地址。接口策略路由的最终目标是实现匹配规则的流按照QoS流策略实现流重定向，同样包括了QoS流策略配置中的以下4项基本配置任务（**需要按顺序配置**），有关QoS流策略的配置方法参见配套图书《华为交换机学习指南》第11章。

① 定义流分类。

② 配置流重定向。

③ 配置流策略。

④ 应用流策略。

在配置接口策略路由前，需要完成以下任务。

① 配置相关接口的IP地址和路由协议，保证路由互通。

② 如果使用ACL作为接口策略路由的流分类规则，配置相应的ACL。

③（可选）SAC（Smart Application Control，智能应用控制）特征库文件已经上传到设备，保存在设备的存储介质中。

15.6.1 定义流分类

定义流分类就是将匹配一定规则的报文归为一类，对匹配同一流分类的报文进行相同的处理，是实现差分服务的前提和基础。流分类是通过 **if-match** 子句进行匹配的，可以基于报文中的内/外层VLAN ID、源IP地址、IP地址、协议类型、DSCP/IP优先级等进行匹配。具体的配置步骤如表15-10所示。

表 15-10　　流分类的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] 例如：[Huawei] **traffic classifier** c1 **operator and**	创建一个流分类，进入流分类视图。命令中的参数和选项说明如下 ● *classifier-name*：指定所创建的流分类名称，1～31 个字符，不支持空格，区分大小写 ● **operator**：可选项，指定流分类下各规则之间的逻辑运算符。如果没有指定本选项，则各规则之间缺省为逻辑“或”的关系 ● **and**：二选一可选项，指定流分类下各规则之间是逻辑“与”的关系。指定该逻辑关系后：当流分类中有 ACL 规则时，报文必须匹配其中一条 ACL 规则，以及所有非 ACL 规则才属于该类；当流分类中没有 ACL 规则时，则报文必须匹配所有非 ACL 规则才属于该类 ● **or**：二选一可选项，指定流分类下各规则之间是逻辑“或”的关系。指定该逻辑关系后，报文只需匹配流分类下的一个，或多个规则就属于该类 缺省情况下，系统上存在名为 default-class 的流分类，（该流分类既不能被删除，也不能对其进行修改），可用 **undo traffic classifier** *classifier-name* 命令删除指定的流分类
以下 **if-match** 匹配规则是并列关系，至少要选择一项，但可以同时配置多项（**以下仅是最常用的匹配规则**）		
3	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] 例如：[Huawei-classifier-c1] **if-match vlan-id** 2	（可选）在流分类中创建基于外层 VLAN ID 进行分类的匹配规则。命令中的参数说明如下 ● *start-vlan-id*：指定起始外层 VLAN ID，取值范围为 1～4 094 的整数 ● **to** *end-vlan-id*：可选参数，指定结束外层 VLAN ID，取值范围为 1～4 094 的整数，但取值一定要大于参数 start-vlan-id 的取值 缺省情况下，流分类中没有基于 VLAN ID 进行分类的匹配规则，可用 **undo if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]命令在流分类中删除指定的基于外层 VLAN ID 进行分类的匹配规则
	if-match cvlan-id *start-vlan-id* [**to** *end-vlan-id*] 例如：[Huawei-classifier-c1] **if-match cvlan-id** 100	（可选）在流分类中创建基于 QinQ 报文内层 VLAN ID 进行分类的匹配规则。命令中的参数参见本表前面介绍的外层 VLAN ID 匹配 **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]命令的对应对数说明，只不过这里是 QinQ 报文中的内层 VLAN ID 缺省情况下，流分类中没有基于 QinQ 报文内层 VLAN ID 进行分类的匹配规则，可用 undo **if-match cvlan-id** *start-cvlan-id* [**to** *end-cvlan-id*]命令在流分类中删除指定的基于 QinQ 报文内层 VLAN ID 进行分类的匹配规则
	if-match 8021p { *8021p-value* } &<1-8> 例如：[Huawei-classifier-c1] **if-match 8021p** 1	（可选）在流分类中创建基于 VLAN 报文的 802.1 p 优先级进行分类的匹配规则。参数 *8021 p-value* 用来指定 VLAN 报文的 802.1 p 优先级值，取值范围为 0～7 的整数，值越大优先级越高。最多可输入 8 个 8 021 p 值 【注意】无论流分类中各规则间关系是“或”还是“与”，执行一次本命令，如果输入多个 8 021 p 值，报文只需匹配其中一个 8 021 p 值就匹配该规则

（续表）

步骤	命令	说明
	if-match 8021p { *8021p-value* } &<1-8> 例如：[Huawei-classifier-c1] **if-match 8021p** 1	本命令为覆盖式命令，即在同一流分类视图下多次配置基于VLAN 报文的 802.1 p 优先级进行流分类的匹配规则后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于 VLAN 报文的 802.1 p 优先级进行分类的匹配规则，可用 **undo if-match 8021p** 命令在流分类中删除基于 VLAN 报文的 802.1 p 优先级进行分类的匹配规则
	if-match cvlan-8021p { *8021p-value* } &<1-8> 例如：[Huawei-classifier-c1] **if-match cvlan-8021p** 1	（可选）在流分类中创建基于 QinQ 报文内层 802.1 p 优先级进行分类的匹配规则。参数 *8021 p-value* 用来指定 QinQ 报文内层的 802.1 p 优先级值，取值范围为 0～7 的整数，值越大优先级越高。最多可输入 8 个 8 021 p 值 【注意】无论流分类中各规则间关系是"或"还是"与"，执行一次本命令，如果输入多个 8 021 p 值，报文只需匹配其中一个 8 021 p 值就匹配该规则 本命令为覆盖式命令，即在同一流分类视图下多次配置基于QinQ 报文内层 802.1 p 优先级进行流分类的匹配规则后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于 QinQ 报文内层 802.1 p 优先级进行分类的匹配规则，可用 **undo if-match cvlan-8021p** 命令在流分类中删除基于 QinQ 报文内层 802.1 p 优先级进行分类的匹配规则
3	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*] 例如：[Huawei-classifier-c1] **if-match destination-mac** 0050-b007-bed3 **mac-address-mask** 00ff-f00f-ffff（匹配目的MAC 地址为 XX50-bXX7-bed3 的报文）	（可选）在流分类中创建基于目的 MAC 地址进行分类的匹配规则。命令中的参数说明如下 ● *mac-address*：指定要匹配的目的 MAC 地址，H-H-H 形式，每个 H 代表 4 位 16 进制数字 ● **mac-address-mask** *mac-address-mask*：可选参数，指定目的 MAC 地址的掩码，H-H-H 形式，每个 H 代表 4 位 16 进制数字，不能为 0-0-0。MAC 地址的掩码作用与 IP 地址的掩码类似，1 表示要匹配该位，0 表示不要匹配该位，可用于确定一组 MAC 地址。用户可以借助 MAC 地址的掩码实现对目的 MAC 地址中某几位进行精确匹配，只需在目的 MAC 地址的掩码中将这几位置 1 【注意】本命令为覆盖式命令，即在同一流分类视图下多次配置基于目的 MAC 地址进行流分类的匹配规则后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于目的 MAC 地址进行分类的匹配规则，可用 **undo if-match destination-mac** 命令在流分类中删除基于目的 MAC 地址进行分类的匹配规则
	if-match source-mac *mac-address* [**mac-address-mask** *mac-address-mask*] 例如：[Huawei-classifier-c1] **if-match source-mac** 0050-ba27-bed5 **mac-address-mask** 00ff-f00f-ffff（匹配源 MAC 地址为 XX50-bXX7-bed5 的报文）	（可选）在流分类中创建基于源 MAC 地址进行分类的匹配规则。命令中的参数参见本表前面匹配 MAC 地址 **if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]命令中的对应参数说明，只不过这里是指源 MAC 地址 【注意】本命令为覆盖式命令，即在同一流分类视图下多次配置基于源 MAC 地址进行流分类的匹配规则后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于源 MAC 地址进行分类的匹配规则，可用 **undo if-match source-mac** 命令在流分类中删除基于源 MAC 地址进行分类的匹配规则

（续表）

步骤	命令	说明
3	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* } 例如：[Huawei-classifier-c1] **if-match l2-protocol arp**	（可选）在流分类中创建基于二层封装的上层协议字段进行分类的匹配规则，对匹配同一流分类的报文进行相同的处理。 命令中的参数和选项说明如下 ● **arp**：多选一选项，指定基于 ARP 协议进行分类，协议类型值为 0x0806 ● **ip**：多选一选项，指定基于 IP 协议进行分类，协议类型值为 0x0800 ● **mpls**：多选一选项，指定基于 MPLS 协议进行分类，协议类型值为 0x8847 ● **rarp**：多选一选项，指定基于 RARP 协议进行分类，协议类型值为 0x8035 【注意】本命令为覆盖式命令，即在同一流分类视图下多次配置基于源 MAC 地址进行流分类的匹配规则后，**仅按最后一次配置生效**。如果包含本命令匹配规则的策略应用到 LAN 接口时，**则仅对 IPv4 报文生效** 缺省情况下，流分类中没有基于二层封装的协议字段进行分类的匹配规则，可用 **undo if-match l2-protocol** 命令在流分类中删除基于二层封装的协议字段进行分类的匹配规则
	if-match any 例如：[Huawei-classifier-c1] **if-match any**	（可选）在流分类中创建基于所有数据报文进行分类的匹配规则。当需要对所有的数据报文作统一的处理时，可以使用本命令匹配所有的数据报文（但不匹配上送 CPU 的控制报文，如 STP 中的 BPDU（Bridge Protocol Data Unit）报文） 【注意】包含本命令匹配规则的策略应用到 LAN 接口时，仅对 IPv4 报文生效 当同一流分类中既有本命令规则，还有其他三层规则时，则本命令仅匹配所有三层报文 缺省情况下，流分类中没有基于所有数据报文进行分类的匹配规则，可用 **undo if-match any** 命令在流分类中删除基于所有数据报文进行分类的匹配规则
	if-match ip-precedence *ip-precedence-value* <1-8> 例如：[Huawei-classifier-class1] **if-match ip-precedence** 1	（可选）在流分类中创建基于 IP 优先级进行分类的匹配规则，参数 *ip-precedence-value* 用来指定要匹配的 IP 优先级值，取值范围为 0～7 的整数，值越大，优先级越高。最多可以配置 8 个 【注意】无论流分类中各规则间关系是“或”还是“与”，执行一次本命令，如果输入多个 IP 值，**报文只需匹配其中一个 IP 值就匹配该规则** 不能在一个逻辑关系为“与”的流分类中同时配置 **if-match dscp** *dscp-value* <1-8>命令和本命令。且本命令为覆盖式命令，即在同一流分类视图下多次执行该命令后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于 IP 优先级进行分类的匹配规则，可用 **undo if-match** *ip-precedence* 命令在流分类中删除基于 IP 优先级进行分类的匹配规则

（续表）

步骤	命令	说明
3	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }* 例如：[Huawei-classifier-c1] **if-match tcp syn-flag psh syn**	（可选）在流分类中创建基于 TCP 报文头中的 SYN Flag 字段进行分类的匹配规则。命令中的选项说明如下 ● **ack**：可多选选项，指定匹配 TCP 报文头中 SYN Flag 字段为 ACK 的报文 ● **fin**：可多选选项，指定匹配 TCP 报文头中 SYN Flag 字段为 FIN 的报文 ● **psh**：可多选选项，指定匹配 TCP 报文头中 SYN Flag 字段为 PSH 的报文 ● **rst**：可多选选项，指定匹配 TCP 报文头中 SYN Flag 字段为 RST 的报文 ● **syn**：可多选选项，指定匹配 TCP 报文头中 SYN Flag 字段为 SYN 的报文 ● **urg**：可多选选项，指定匹配 TCP 报文头中 SYN Flag 字段为 URG 的报文 【注意】包含本命令匹配规则的策略应用到 LAN 接口时，仅对 IPv4 报文生效 本命令为覆盖式命令，即在同一流分类视图下多次执行该命令后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于 TCP 报文头中的 SYN Flag 进行分类的匹配规则，可用 **undo if-match tcp** 命令在流分类中删除基于 TCP 报文头中的 SYN Flag 进行分类的匹配规则
	if-match inbound-interface *interface-type interface-number* 例如：[Huawei-classifier-class1]**if-match inbound-interface** ethernet 2/0/0	（可选）在流分类中创建基于入接口对报文进行分类的匹配规则 【注意】设备仅支持在 WAN 接口应用包含该匹配规则的流策略。**当包含此匹配规则的流策略应用在 WAN 接口出方向时，匹配的入接口不得为子接口或 Eth-Trunk 的成员接口** 本命令为覆盖式命令，即在同一流分类视图下多次执行该命令后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于入接口对报文进行分类的匹配规则，可用 **undo if-match inbound-interface** 命令在流分类中删除基于入接口对报文进行分类的匹配规则
	if-match outbound-interface *interface-type interface-number:channel* 例如：[Huawei-classifier-class1]**if-match outbound-interface** Cellular 3/0/0:1	（可选）在流分类中创建基于 Cellular 出通道口对报文进行分类的匹配规则 【注意】本命令为覆盖式命令，即在同一流分类视图下多次执行该命令后，**仅按最后一次配置生效** 缺省情况下，流分类中没有基于 Cellular 出通道口对报文进行分类的匹配规则，**undo if-match outbound-interface** 命令在流分类中删除基于 Cellular 出通道口对报文进行分类的匹配规则
	if-match acl { *acl-number* | *acl-name* } 例如：[Huawei-classifier-c1] **if-match acl** 2046	（可选）在流分类中创建基于 ACL 进行分类的匹配规则。命令中的参数说明如下 ● *acl-number*：二选一参数，指定 ACL 的编号，取值范围为 2 000～4 999 的整数，可以是基本 ACL、高级 ACL 和二层 ACL ● *acl-name*：二选一参数，指定 ACL 的名称，1～32 个字符，不支持空格，区分大小写，可以是英文字母、数字和“#”、“%”、“-”等字符的组合，但必须以英文字母 a～z 或 A～Z 开始

（续表）

步骤	命令	说明
3	**if-match acl** { *acl-number* | *acl-name* } 例如：[Huawei-classifier-c1] **if-match acl** 2046	【注意】无论流分类中各规则间关系是“或”还是“与”，执行一次本命令，如果某 ACL 规则中有多个 rule，报文只需匹配其中一个 rule 就匹配该 ACL 规则。可以在一条流分类中配置多个 ACL 以匹配不同的报文 当使用 ACL 作为流分类规则匹配源 IP 地址时，通过在接口下的 **qos pre-nat** 命令配置 NAT 预分类功能，可以将 NAT 转换前的私网 IP 地址信息携带到出接口，即可实现基于私网 IP 地址的分类，从而对来自不同私网 IP 地址的报文提供差分服务 缺省情况下，流分类中没有基于 ACL 进行分类的匹配规则，可用 **undo if-match acl** { *acl-number* | *acl-name* }命令删除指定的基于 ACL 进行分类的匹配规则

15.6.2 配置流重定向

配置流重定向就是配置 QoS 流策略的一种流行为。通过配置重定向，设备将符合流分类规则的报文重定向到指定的下一跳地址或指定接口。**但包含重定向动作的流策略只能在接口的入方向上应用。**

可以通过与 NQA 联动，在网络链路出现故障时，实现路由快速切换，保障数据流量正常转发，因为 NQA 是网络故障诊断和定位的有效工具。与 NQA 实现联动后有以下两种情况。

① 当 NQA 检测到与目的 IP 可达时，按照指定的 IP 进行报文转发，即重定向生效。

② 当 NQA 检测到与目的 IP 不可达时，系统将按原来的转发路径转发报文，即重定向不生效。

配置流重定向的步骤如表 15-11 所示。

表 15-11　流重定向的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**traffic behavior** *behavior-name* 例如：[Huawei] **traffic behavior** b1	创建一个流行为，进入流行为视图。参数 *behavior-name* 用来指定所创建的流行为名称，1～31 个字符，不支持空格，区分大小写 【说明】系统上缺省存在名为 **be** 的流行为，该流行为既不能被删除，也不能对其进行修改 创建流分类是为了提供差分服务，它必须与某些流量控制或资源分配动作（比如报文过滤、流量监管、重标记等）关联起来才有意义，而这些具体流动作的总和便构成了流行为。一个设备上最多可以配置的流行为个数为 1 024，且一个流行为中可以包含多个流动作 缺省情况下，系统上存在名为 **be** 的流行为，可用 **undo traffic behavior** *behavior-name* 命令删除指定的流行为。如果要删除某个流行为，必须先取消包含该流行为的流策略在接口上的应用，并且在流策略下解除流分类和流行为的绑定。**如果只是修改某个流行为所包含的流动作，就不需要取消包含该流行为的流策略在接口上的应用**

（续表）

步骤	命令	说明
3	**redirect ip-nexthop** *ip-address* [**track nqa** *admin-name test-name*] 例如：[Huawei-behavior-b1] **redirect ip-nexthop** 10.0.0.1	（二选一）将符合流分类的报文重定向到下一跳，并配置重定向与 NQA 测试例联动。命令中的参数说明如下 • *ip-address*：指定下一跳的 IP 地址。如果设备上没有命令中下一跳 IP 地址对应的 ARP 表项，设备会触发 ARP 学习，如果一直学习不到 ARP，则重定向不生效 • **nqa** *admin-name test-name*：可选参数，指定与重定向联动的 NQA 测试例。其中：*admin-name* 用来创建的 NQA 测试例管理者的名称，1～32 个字符，不支持空格，区分大小写；*test-name* 用来指定要进行联动的 NQA 测试例的名称，1～32 个字符，不支持空格，区分大小写 缺省情况下，流行为中没有将报文重定向到单个下一跳 IP 地址的动作，可用 **undo redirect** 命令删除重定向配置
	redirect interface *interface-type interface-number* 例如：[Huawei-behavior-b1] **redirect interface** cellular 0/0/1	（二选一）将符合流分类的报文重定向到指定接口。**目前设备仅支持重定向到 3G 接口和 Dialer 接口，且包含重定向动作的流策略只能在接口的入方向上应用** 缺省情况下，流行为中没有将报文重定向到指定接口的动作，可用 **undo redirect** 命令在流行为中删除重定向配置

15.6.3 配置并应用流策略

流策略就是将以上两节配置的流分类和流行为关联起来，而流策略应用是将配置好的流策略在对应的接口入，或者出方向上应用，分别对进入该接口，或者从该接口转发的数据报文应用流策略。具体的配置步骤如表 15-12 所示。

表 15-12　　流策略配置与应用的配置步骤

步骤	命令	说明
1	**system-view** 例如：<Huawei> **system-view**	进入系统视图
2	**traffic policy** *policy-name* 例如：[Huawei]**traffic policy** p1	创建一个流策略，并进入流策略视图。参数 *policy-name* 用来指定所创建的流策略名称，1～31 个字符，不支持空格，区分大小写 缺省情况下，系统未创建任何流策略，可用 **undo traffic policy** *policy-name* 命令删除指定的流策略。但如果需要删除的流策略已经应用到接口，则不允许直接删除该策略，需要先在相应的接口视图下执行 **undo traffic-policy** 命令取消对该策略的应用，然后到系统视图下执行 **undo traffic policy** *policy-name* 命令完成指定流策略的删除。如果该流策略还没有应用到接口上，则可以直接删除
3	**classifier** *classifier-name* behavior *behavior-name* 例如：[Huawei-trafficpolicy-p1] **classifier** c1 **behavior** b1	在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。命令中的参数说明如下 • *classifier-name*：指定要关联的流分类的名称 • *behavior-name*：指定要关联的流行为的名称 目前，设备最多可以配置的流分类、流行为以及流策略数目均为 1 024 个。**在单个流策略下，每个流分类只能与一个流行为关联**，每个流策略支持 1 024 个流分类和流行为的绑定 缺省情况下，流策略中没有绑定流分类和流行为，可用 **undo classifier** *classifier-name* 命令在流策略中取消指定的流分类和流行为的绑定

（续表）

步骤	命令	说明
4	**quit** 例如：[Huawei-trafficpolicy-p1] **quit**	退出流策略视图，返回系统视图
5	**interface** *interface-type interface-number* [.*subinterface-number*] 例如：[Huawei] **interface** ethernet 2/0/0	键入要应用流策略的接口，或子接口，进入接口视图
6	**traffic-policy** *policy-name* { **inbound** | **outbound** } 例如：[Huawei-Ethernet2/0/0] **traffic-policy** p1 **inbound**	在接口或子接口的入方向或出方向应用流策略。命令中的参数和选项说明如下 ● *policy-name*：指定要应用的流策略的名称 ● **inbound**：二选一选项，指定在接口入方向上应用由参数 *policy-name* 指定的流策略 ● **outbound**：二选一选项，指定在接口出方向上应用由参数 *policy-name* 指定的流策略 【注意】**每个接口的同一个方向上能且只能应用一个流策略**，但同一个流策略可以同时应用在不同接口的不同方向 **流策略一旦应用后，不允许直接删除该流策略及其包含的流分类或流行为**，如果要删除已经在接口下应用的流策略，则必须首先在接口下执行 **undo traffic-policy** [*policy-name*] { **inbound** | **outbound** }命令取消对该策略的应用，然后到系统视图下执行**undo traffic policy** *policy-name* 命令删除该策略 缺省情况下，接口上没有应用任何流策略，可用 **undo traffic-policy** [*policy-name*] { **inbound** | **outbound** }命令取消在接口上应用指定的流策略

15.6.4 接口策略路由管理

配置好以上接口策略路由后，可以通过以下 **display** 视图命令查看相关配置，验证配置结果。

① **display traffic classifier user-defined** [*classifier-name*]：查看设备上所有或者指定的流分类信息。

② **display acl** { **name** *acl-name* | *acl-number* | all }：查看指定的 ACL 规则的配置信息。

③ **display acl resource** [**slot** *slot-id*]：查看所有或者指定主控板上的 ACL 规则的资源信息。

④ **display traffic policy user-defined** [*policy-name* [classifier *classifier-name*]]：查看所有或者指定的流策略的配置信息。

⑤ **display traffic-policy applied-record** *policy-name*：查看指定流策略的应用记录信息。

⑥ **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]：查看所有或者指定的流行为的配置信息。

15.6.5 接口策略路由配置示例

本示例的基本拓扑结构如图 15-7 所示，VLAN10 和 VLAN20 是企业内部的两个部门，分别通过交换机连接到 RouterA 的 GE1/0/0 和 GE2/0/0。

HOSTA 和 HOSTB 是同一部门内的两台主机，IP 地址分别为 192.168.1.2/24 和

192.168.1.3/24，属于 192.168.1.0/24 网段；HOSTC 和 HOSTD 是另一部门的两台主机，IP 地址分别为 192.168.2.2/24 和 192.168.2.3/24，属于 192.168.2.0/24 网段。RouterA 有两条链路连接到 Internet，它们是 RouterA→RouterB→RouterD 和 RouterA→RouterC→RouterD。各路由器接口的 IP 地址如表 15-13 所示。现有如下要求。

① 当 RouterA 的两条连接到 Internet 的链路都正常时，企业内部不同网段地址的报文通过不同的链路连接到 Internet。

② 当一条链路发生故障时，企业内部不同网段地址的报文都走无故障的链路，避免长时间的业务中断；而当故障链路恢复后，恢复报文从不同链路连接到 Internet。

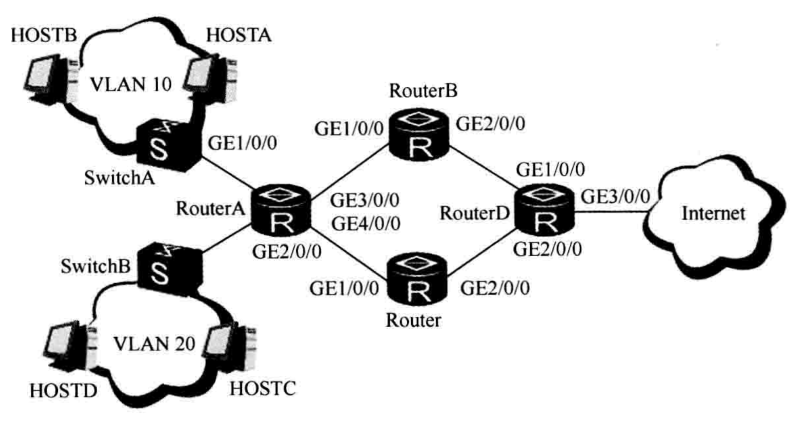


图 15-7 接口策略路由配置示例拓扑结构

表 15-13 示例中各路由器接口的 IP 地址

设备	接口	IP 地址
RouterA	GE1/0/0	192.168.1.1/24
	GE2/0/0	192.168.2.1/24
	GE3/0/0	192.168.3.1/24
	GE4/0/0	192.168.4.1/24
RouterB	GE1/0/0	192.168.3.2/24
	GE2/0/0	192.168.5.2/24
RouterC	GE1/0/0	192.168.4.2/24
	GE2/0/0	192.168.6.2/24
RouterD	GE1/0/0	192.168.5.1/24
	GE2/0/0	192.168.6.1/24
	GE3/0/0	192.168.7.1/24

1. 基本配置思路分析

根据本示例的要求，可以考虑采用流重定向与 NQA 联动，实现在被监控的链路正常时按照流策略定义的重定向行为对流进行重定向转发，而当被监控的链路出现故障时，按照路由表中的路由进行转发。但是这里又涉及一个问题，那就是当链路出现故障时，IP 路由表中的路由表项不会立即清除，所以又需要利用路由与 NQA 的联动功能及时删除对应的路由表项（在链路由故障恢复后，该路由又会重新添加到 IP 路由表中）。本示例采用静态路由与 NQA 联动的方式（具体参见第 10 章）。

本示例的具体配置思路如下。

① 配置各设备接口 IP 地址及路由协议，使企业用户能通过 RouterA 访问 Internet。

② 配置 NQA 测试例，检测链路 RouterA→RouterB→RouterD 和 RouterA→RouterC→RouterD 是否正常。

③ 配置 NQA 和静态路由联动，实现当链路故障时，及时删除路由表中对应路由表项，使流量可以切换到正常链路。

④ 配置流分类，匹配规则为匹配报文的源 IP 地址，实现基于源地址对报文进行分类。

⑤ 配置流行为，即配置 NQA 与流重定向联动，实现当 NQA 测试例检测到链路 RouterA→RouterB→RouterD 正常时，将满足规则的报文重定向到 192.168.3.2/24，当 NQA 测试例检测到链路 RouterA→RouterC→RouterD 正常时，将满足规则的报文重定向到 192.168.4.2/24。

⑥ 配置流策略，绑定上述流分类和流行为，并应用到相应的接口，实现策略路由。

2. 具体配置步骤

① 按照表 15-13 所示注的各设备接口 IP 地址，配置各设备接口的 IP 地址。下面仅以 RouterA 为例进行介绍，其他设备的配置方法一样，略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.2.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.3.1 24
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] interface gigabitethernet 4/0/0
[RouterA-GigabitEthernet4/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet4/0/0] quit
```

② 配置各设备间的静态路由。注意，静态路由具有单向性和接力性，必须在各设备上确保双向通信都有所需的连续静态路由。

```
[RouterA] ip route-static 192.168.7.0 255.255.255.0 192.168.3.2
[RouterA] ip route-static 192.168.7.0 255.255.255.0 192.168.4.2
[RouterA] ip route-static 192.168.5.0 255.255.255.0 192.168.3.2
[RouterA] ip route-static 192.168.6.0 255.255.255.0 192.168.4.2

[RouterB] ip route-static 192.168.7.0 255.255.255.0 192.168.5.1
[RouterB] ip route-static 192.168.1.0 255.255.255.0 192.168.3.1
[RouterB] ip route-static 192.168.2.0 255.255.255.0 192.168.3.1

[RouterC] ip route-static 192.168.7.0 255.255.255.0 192.168.6.1
[RouterC] ip route-static 192.168.1.0 255.255.255.0 192.168.4.1
[RouterC] ip route-static 192.168.2.0 255.255.255.0 192.168.4.1

[RouterD] ip route-static 192.168.1.0 255.255.255.0 192.168.5.2
[RouterD] ip route-static 192.168.1.0 255.255.255.0 192.168.6.2
[RouterD] ip route-static 192.168.2.0 255.255.255.0 192.168.6.2
[RouterD] ip route-static 192.168.2.0 255.255.255.0 192.168.5.2
[RouterD] ip route-static 192.168.3.0 255.255.255.0 192.168.5.2
[RouterD] ip route-static 192.168.4.0 255.255.255.0 192.168.6.2
```

③ 在 RouterA 和 RouterD 的两条链路之间分别配置 NQA 测试例。

在 RouterA 上要配置测试到达 RouterD 的 GE1/0/0 接口和 GE2/0/0 接口的两个 NQA 测试实例，所创建的管理者账户都是 admin，实例名分别为 vlan10 和 vlan20。

```
[RouterA] nqa test-instance admin vlan10        !---创建一个NQA测试实例，并创建管理者帐户为admin，实例名称为vlan10
[RouterA-nqa-admin-vlan10] test-type icmp       !---配置 NQA 测试例的测试类型为 ICMP，即通过 ping 操作进行测试
[RouterA-nqa-admin-vlan10] destination-address ipv4 192.168.5.1   !---指定测试实例的目的地址，也就是进行 ping 操作
```

```
的目的地址，本示例中为 RouterD 的 GE1/0/0 接口 IP 地址
    [RouterA-nqa-admin-vlan10] frequency 10                          !---指定连续两次探测间的时间间隔为 10 秒
    [RouterA-nqa-admin-vlan10] probe-count 2                         !---指定一次探测进行的测试次数
    [RouterA-nqa-admin-vlan10] start now                             !--- 指定立即启动执行当前测试例
    [RouterA-nqa-admin-vlan10] quit
    [RouterA] nqa test-instance admin vlan20
    [RouterA-nqa-admin-vlan20] test-type icmp
    [RouterA-nqa-admin-vlan20] destination-address ipv4 192.168.6.1
    [RouterA-nqa-admin-vlan20] frequency 10
    [RouterA-nqa-admin-vlan20] probe-count 2
    [RouterA-nqa-admin-vlan20] start now
    [RouterA-nqa-admin-vlan20] quit
```

在 RouterD 上要配置测试到达 RouterA 的 GE3/0/0 接口和 GE4/0/0 接口的两个 NQA 测试实例，所创建的管理者账户都是 admin，实例名分别为 vlan10 和 vlan20。

RouterD 上的配置：

```
[RouterD] nqa test-instance admin vlan10
[RouterD-nqa-admin-vlan10] test-type icmp
[RouterD-nqa-admin-vlan10] destination-address ipv4 192.168.3.1
[RouterD-nqa-admin-vlan10] frequency 10
[RouterD-nqa-admin-vlan10] probe-count 2
[RouterD-nqa-admin-vlan10] start now
[RouterD-nqa-admin-vlan10] quit
[RouterD] nqa test-instance admin vlan20
[RouterD-nqa-admin-vlan20] test-type icmp
[RouterD-nqa-admin-vlan20] destination-address ipv4 192.168.4.1
[RouterD-nqa-admin-vlan20] frequency 10
[RouterD-nqa-admin-vlan20] probe-count 2
[RouterD-nqa-admin-vlan20] start now
[RouterD-nqa-admin-vlan20] quit
```

④ 在 RouterA 和 RouterD 上分别配置与对应 NQA 测试实例联动、到达目的网络的静态路由。通过配置静态路由与 NQA 联动，可以实现在链路发生故障后，NQA 测试例快速地检测到链路的变化，并且在 IP 路由表中把与该 NQA 测试例联动的静态路由删除，从而影响流量转发的目的。注意，在配置静态路由与 NQA 联动时，选择的测试实例名称一定要与静态路由对应的链路一致。

RouterA 上的配置如下。

```
    [RouterA] ip route-static 192.168.7.1 255.255.255.0 192.168.3.2 track nqa admin vlan10 !---配置 RouterA 经由 RouterB
到达 RouterD GE3/0/0 接口的 NQA 与静态路由联动
    [RouterA] ip route-static 192.168.7.1 255.255.255.0 192.168.4.2 track nqa admin vlan20 !---配置 RouterA 经由 RouterC
到达 RouterD GE3/0/0 接口的 NQA 与静态路由联动
    [RouterA] quit
```

RouterD 上的配置如下。

```
    [RouterD] ip route-static 192.168.1.0 255.255.255.0 192.168.5.2 track nqa admin vlan10 !---配置 RouterD 经由 RouterB
到达 RouterA GE1/0/0 接口所在网络的 NQA 与静态路由联动
    [RouterD] ip route-static 192.168.1.0 255.255.255.0 192.168.6.2 track nqa admin vlan20 !---配置 RouterD 经由 RouterC
到达 RouterA GE1/0/0 接口所在网络的 NQA 与静态路由联动
    [RouterD] ip route-static 192.168.2.0 255.255.255.0 192.168.5.2 track nqa admin vlan10 !---配置 RouterD 经由 RouterB
到达 RouterA GE2/0/0 接口所在网络的 NQA 与静态路由联动
    [RouterD] ip route-static 192.168.2.0 255.255.255.0 192.168.6.2 track nqa admin vlan20 !---配置 RouterD 经由 RouterC
到达 RouterA GE2/0/0 接口所在网络的 NQA 与静态路由联动
    [RouterD] quit
```

⑤ 在 RouterA 和 RouterD 上分别配置流分类。因为通信是双向的，所以需要在双向进行配置流策略，以便指导对应方向的流按规定进行重定向。

在 RouterA 上创建流分类 vlan10、vlan20，通过基本 ACL 分别匹配源地址为 192.168.1.0/24 和 192.168.2.0/24 网段（分别对应 VLAN10 和 VLAN 20 所在的网段）的报文。

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule 10 permit source 192.168.1.0 0.0.0.255
[RouterA-acl-basic-2000] quit
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule 20 permit source 192.168.2.0 0.0.0.255
[RouterA-acl-basic-2001] quit
[RouterA] traffic classifier vlan10
[RouterA-classifier-vlan10] if-match acl 2000
[RouterA-classifier-vlan10] quit
[RouterA] traffic classifier vlan20
[RouterA-classifier-vlan20] if-match acl 2001
[RouterA-classifier-vlan20] quit
```

在 RouterD 上创建流分类 vlan10、vlan20，通过高级 ACL 分别匹配目的地址为 192.168.1.0/24 和 192.168.2.0/24 网段的报文。

```
[RouterD] acl number 3000
[RouterD-acl-adv-3000] rule 10 permit ip destination 192.168.1.0 0.0.0.255
[RouterD-acl-adv-3000] quit
[RouterD] acl number 3001
[RouterD-acl-adv-3001] rule 20 permit ip destination 192.168.2.0 0.0.0.255
[RouterD-acl-adv-3001] quit
[RouterD] traffic classifier vlan10
[RouterD-classifier-vlan10] if-match acl 3000
[RouterD-classifier-vlan10] quit
[RouterD] traffic classifier vlan20
[RouterD-classifier-vlan20] if-match acl 3001
[RouterD-classifier-vlan20] quit
```

⑥ 在 RouterA 和 RouterD 上分别配置流重向行为。这样，当 NQA 测试例检测到链路正常时，按照流策略定义的行为进行流重定向；而 NQA 测试例检测到链路故障时，则要按照路由表中的有效路由进行报文转发。

在 RouterA 上创建流行为 vlan10，配置 NQA 测试例 admin vlan10 与重定向到下一跳 192.168.3.2/24 联动，实现在该下一跳链路正常时把数据从该链路上转发的目的。

```
[RouterA] traffic behavior vlan10
[RouterA-behavior-vlan10] redirect ip-nexthop 192.168.3.2 track nqa admin vlan10
[RouterA-behavior-vlan10] quit
```

在 RouterA 上创建流行为 vlan20，配置 NQA 测试例 admin vlan20 与重定向到下一跳 192.168.4.2/24 联动，实现在该下一跳链路正常时把数据从该链路上转发的目的。

```
[RouterA] traffic behavior vlan20
[RouterA-behavior-vlan20] redirect ip-nexthop 192.168.4.2 track nqa admin vlan20
[RouterA-behavior-vlan20] quit
```

在 RouterD 上创建流行为 vlan10，配置 NQA 测试例 admin vlan10 与重定向到下一跳 192.168.5.2/24 联动，实现在该下一跳链路正常时把数据从该链路上转发的目的。

```
[RouterD] traffic behavior vlan10
[RouterD-behavior-vlan10] redirect ip-nexthop 192.168.5.2 track nqa admin vlan10
[RouterD-behavior-vlan10] quit
```

在 RouterD 上创建流行为 vlan20，配置 NQA 测试例 admin vlan20 与重定向到下一跳 192.168.6.2/24 联动，实现在该下一跳链路正常时把数据从该链路上转发的目的。

```
[RouterD] traffic behavior vlan20
[RouterD-behavior-vlan20] redirect ip-nexthop 192.168.6.2 track nqa admin vlan20
[RouterD-behavior-vlan20] quit
```

⑦ 在 RouterA 和 RouterD 上分别配置流策略并应用到接口上。

在 RouterA 上创建流策略 vlan10、vlan20，分别将流对应的流分类和流行为进行绑定，并将流策略 vlan10 应用到接口 GE1/0/0 入方向，将流策略 vlan20 应用到接口 GE2/0/0 入方向。

```
[RouterA] traffic policy vlan10
[RouterA-trafficpolicy-vlan10] classifier vlan10 behavior vlan10
[RouterA-trafficpolicy-vlan10] quit
[RouterA] traffic policy vlan20
[RouterA-trafficpolicy-vlan20] classifier vlan20 behavior vlan20
[RouterA-trafficpolicy-vlan20] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] traffic-policy vlan10 inbound
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] traffic-policy vlan20 inbound
[RouterA-GigabitEthernet2/0/0] quit
```

在 RouterD 上创建流策略 vlan10，将两个流分类和对应的流行为进行绑定，并将流策略 vlan10 应用到接口 GE3/0/0 入方向。

```
[RouterD] traffic policy vlan10
[RouterD-trafficpolicy-vlan10] classifier vlan10 behavior vlan10
[RouterD-trafficpolicy-vlan10] classifier vlan20 behavior vlan20
[RouterD-trafficpolicy-vlan10] quit
[RouterD] interface gigabitethernet 3/0/0
[RouterD-GigabitEthernet3/0/0] traffic-policy vlan10 inbound
[RouterD-GigabitEthernet3/0/0] quit
```

配置好后，下面可以通过 **display this** 接口视图命令查看相应接口配置，验证配置结果。下面是 RouterA GE1/0/0 和 GE2/0/0 接口上的配置信息。可以看到，它们所应用的流策略（**参见输出信息中的粗体字部分**）。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] display this
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 traffic-policy vlan10 inbound
#
return
[RouterA-GigabitEthernet1/0/0] quit

[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] display this
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
 traffic-policy vlan20 inbound
#
return
[RouterA-GigabitEthernet2/0/0] quit
```

也可以通过 **display traffic policy user-defined** 任意视图命令查看 RouterA 和 RouterD 上用户自定义的流策略的配置信息。下面是 RouterA 上的配置。

```
[RouterA] display traffic policy user-defined
 User Defined Traffic Policy Information:
 Policy: vlan10
  Classifier: vlan10
   Operator: OR
    Behavior: vlan10
     Redirect:
       Redirect ip-nexthop 192.168.3.2 track nqa admin vlan10

 Policy: vlan20
  Classifier: vlan20
   Operator: OR
    Behavior: vlan20
     Redirect:
       Redirect ip-nexthop 192.168.4.2 track nqa admin vlan20
```

封面设计：Dile迪利

《华为路由器学习指南》是由华为公司组织编写的一本具有权威性的华为路由器产品学习工具图书，也是华为ICT认证系列培训教材。本书以华为最新的AR G3系列企业级路由器为主线，全面介绍了AR G3系列路由器各种功能的配置与管理方法。

本书集系统性、专业性和实用性于一体，既有全面、深入且富有经验性的各种技术实现原理的剖析，又有以Step-by-Step方式的详尽配置步骤的介绍，条理清晰，繁而不杂，一学即会。并且通过大量典型功能应用配置示例，对各种功能配置任务或配置思路进行深入分析，使理论和实践完美结合，学以致用，化繁为简。







分类建议：计算机网络 / 路由选择
人民邮电出版社网址：www.ptpress.com.cn

ISBN 978-7-115-35742-7
定价：149.00 元